Using Bayesian Networks to represent Parameterised Risk Models for the UK Railways

George Joseph Bearfield

Submitted for the degree of Doctor of Philosophy

Queen Mary, University of London

Department of Computer Science

Table of figures

Table of tables

Author's declaration

All of the work presented in this thesis represents the original contribution of the author. Some of the material presented in this thesis has previously been presented as part of the following publications:

1. D W R Marsh and G Bearfield, Generalizing event trees using Bayesian networks, in Proc. IMechE, PartO: J. Risk and Reliability, 222(O2), 105-114, 2008.

2. Marsh D.W.R. and Bearfield, G. J. Representing Parameterised Fault Trees using Bayesian Networks, In F. Saglietti, and N. Oster (eds.), Proceedings of the 26th International Conference on Computer Safety, Reliability and Security, SAFECOMP 2007, LNCS 4680, 120-133, 2007.

3. Bearfield G.J., Dray P.A. and Marsh D.W.R. Constructing Scalable and Parameterised System Wide Risk Models, in Proceedings of 25th International System Safety Conference, Baltimore, USA, August 13-17, 2007, System Safety Society, 2007.

4. Marsh D.W.R. and Bearfield, G.J. Merging Event Trees Using Bayesian Networks. In Proceedings of ESREL 2007, Stavanger Norway. T. Aven and J. E. Vinnem (Eds). Taylor & Francis. p.1489-1496. (Selected for the Journal of Risk and Reliability Special Issue of Selected Papers from ESREL 2007).

5. Bearfield, G. J. Achieving clarity in the requirements and practice for taking safety decisions in the railway industry in Great Britain". In Proceedings of ESREL 2007, Stavanger, Norway. T. Aven and J. E. Vinnem (Eds). Taylor & Francis. p.559-564.

6. Bearfield G.J. and Marsh D.W.R. Generalising Event Trees using Bayesian Networks with a Case Study of Train Derailment, In R. Winther, B.A. Gran, and G. Dahll (eds.), Proceedings of the 24th International Conference on Computer Safety, Reliability and Security, SAFECOMP 2005, LNCS 3688, 52-66, 2005.

7. William Marsh & George Bearfield, "Using Bayesian Networks to Model Accident Causation in the GB Railway Industry" in Probabilistic Safety Assessment and Management (PSAM7-ESREL'04): Proceedings of the 7th International Conference on Probabilistic Safety Assessment and Management, 14-18 June 2004, Berlin, Germany, 2004

Abstract

The techniques currently used to model risk and manage the safety of the UK railway network are not aligned to the mechanism by which catastrophic accidents occur in this industry. In this thesis, a new risk modelling method is proposed to resolve this problem.

Catastrophic accidents can occur as the result of multiple failures occurring to all of the various defences put in place to prevent them. The UK railway industry is prone to this mechanism of accident occurrence, as many different technical, operational and organizational defences are used to prevent accidents.

The railway network exists over a wide geographic area, with similar accidents possible at many different locations. The risk from these accidents is extremely variable and depends on the underlying conditions at each particular location, such as the state of assets or the speed of trains. When unfavourable conditions coincide the probability of multiple failures of planned defences increases and a 'risk hotspot' arises.

Ideal requirements for modelling risk are proposed, taking account of the need to manage multiple defences of conceptually different type and the existence of risk hotspots. The requirements are not met by current risk modelling techniques although some of the requirements have been addressed experimentally, and in other industries and countries.

It is proposed to meet these requirements using Bayesian Networks to supplement and extend fault and event tree analysis, the traditional techniques used for risk modelling in the UK railway industry. Application of the method is demonstrated using a case study: the building of a model of derailment risk on the UK railway network.

The proposed method provides a means of better integrating industry wide analysis and risk modelling with the safety management tasks and safety related decisions that are undertaken by safety managers in the industry.

1 Introduction

1.1 Safety of complex systems

In the modern world, our safety depends on complex systems. We travel by aeroplane to go on holiday and commute to work using the railway; we use energy that is derived from nuclear power stations; and we use products which are developed using chemical processing. Each of these systems comprises different elements. There is a technological core, generally consisting of engineered hardware and software systems; there are people who maintain and operate the technological parts of the system; and there is the management organisation which sets the context and culture in which the whole system functions.

These systems have the potential for catastrophe, but society demands high levels of safety from them. In order to meet society's needs, they must be designed, operated, maintained and managed to ensure that the occurrence of accidents is reduced as much as possible. Potential accidents must be predicted and the whole system made to operate in such a way as to prevent them from occurring.

In most industries, a clear understanding of which accidents are possible has arisen over many years through experience. This understanding of accidents, including their causes, relative severities and likelihoods, is consolidated and captured in risk models. These models are widely used and accepted. They are used to support decisions about how to design, operate and manage the system and support the management systems that companies have in place for ensuring safety. Both the accuracy of risk models, and the way in which they influence decision making and safety management, are critical to the safe operation of complex systems.

1.2 The UK railway system

The railway industry in the United Kingdom[1] (UK) is one such complex system. It is huge in scope, consisting of many thousands of miles of rail and many stations and depots. It also comprises of a variety of different hardware and software systems, including those for signalling, electrification and rolling stock. These elements must be

---

[1] The railway network in Northern Ireland is undertaken under a separate managerial and legislative framework from that of the remainder of the United Kingdom; however, this is not relevant to the work described here so for the sake of familiarity the UK is referred to in this thesis rather than Great Britain.

integrated and the system must be operated, maintained and managed effectively to deliver a safe transport service to the railway's many users.

Safety is assured through the use of various control measures. The system is designed so that no single failure or error in control measures can lead to an accident. The technical, operational and managerial elements of the system all play their part in preventing accidents and must work together to ensure that accidents do not occur. This makes the system prone to major accidents when all controls fail coincidentally in the same location. Safety is a property of the system as a whole. However the safety controls are often implemented by conceptually different, and separately managed, engineering and operational disciplines. Because of the complexity that this creates management of safety is difficult. Local conditions may mean that the risk in a particular location is disproportionately high, because of the increased likelihood of failure of a number of safety controls. However detailed knowledge of the potential accidents and the effectiveness of each safety control in each location is needed to identify such conditions before an accident occurs.

The UK Railway Industry was privatised in 1994. Since privatisation the industry has increasingly moved away from a prescriptive, standards-based approach to safety management. The modern railway industry relies increasingly on risk models and risk assessment practices. Safety has improved in recent years but serious train accidents have continued to occur. The industry must therefore seek to improve safety by developing better techniques for estimating accident risk, and by using these estimates to support decision making more effectively.

1.3 Risk modelling in the UK railway industry

If a company understands what the various diffuse causes of an accident are, and where they are likely to occur, it can seek to ensure that safety controls prevent their occurrence.

The railway industry's understanding of accident causation is captured in risk models. However, the approaches used are not well aligned to the nature of risk on the railway. Models do not include the myriad causes that might be implicated in the occurrence of a major accident. Risk models are also often representative of large sections of the network, or use data derived in this way. Therefore they do not capture the specific circumstances that often result in substantially increased risk in a particular situation. For example, at Ladbroke Grove an accident occurred when an inexperienced train driver drove a train past a red signal on a section of the network where experienced

drivers had noted the difficulty of reading and interpreting the meaning of lineside signals (Cullen 2000; Cullen 2001). The increased risk at this location was not estimated prior to the accident as there were no risk models which explicitly included both driver inexperience and poorly positioned infrastructure as potential accident causes. Even if these conditions had been included as causes in a model, it is unlikely that the high level of risk would have been identified as it occurred in this particular situation only, and any risk assessment undertaken would be likely to model the average risk across a particular area of infrastructure and an average set of circumstances. The Ladbroke Grove accident is described and investigated further in section 3.3.

According to the theory of organizational accidents (Reason 2002), in the aftermath of an accident there is increased awareness and vigilance throughout an organisation and safety performance improves as a result. Catastrophic accidents are rare. In the absence of accidents, risk levels will gradually rise as an organisation becomes complacent.

In this thesis I argue that the UK railway industry is prone to the occurrence of organizational accidents. However, the nature of risk on a rail network means that the industry faces particular problems in managing such risk, and preventing the occurrence of major accidents. The railway network exists over a wide geographic area. Similar accidents are thus possible at many different locations. However, the risk from these accidents is extremely variable and depends on the underlying conditions at each particular location. The implication of this large system scope and variation, and organizational accident theory is that, at any given time, there are locations on the railway network where risk is disproportionately high. This huge scope and variation complicates risk modelling, and the review presented finds that current approaches do not easily support systematic estimation of risk across a range of locations.

Risk models which include all significant accident causes, and which are rapidly updatable with different situation specific information, could be used to identify when and where risk levels are dangerously high to pre-empt the occurrence of accidents. This would lead to a more intelligent and targeted approach to the management of safety, and models which better support decision making.

1.4 Hypotheses

Four linked hypotheses are argued in this thesis.

Hypothesis 1:

Organizational accident theory provides an explanation for the mechanisms by which major accidents occur within the UK railway industry.

Hypothesis 2:

Given that the industry is prone to the occurrence of organizational accidents a risk modelling approach with particular characteristics is needed in order to ideally support the effective management of safety (these particular characteristics are defined as requirements RMR1-3, SMS1 and SDM1 in section 3.7)

Hypothesis 3:

Current risk modelling approaches in use in the UK railway industry do not have these characteristics.

Hypothesis 4:

The development of a risk modelling approach that has these characteristics is possible.

1.5 Outline

The thesis is structured as follows:

Chapter 2 provides essential context required to understand the remainder of the thesis. Concepts relating to risk analysis, risk modelling, safety management and their general application in the UK railway industry are first described. Because many terms are subjective and their use is flexible, the terms that are used in the remainder of this thesis are selected and definitions provided for them. In particular the term 'cause' is defined and a number of different categorisations of causal type are proposed. The modelling and analysis techniques that are commonly used in the railway industry are also described.

In Chapter 3 organizational accident theory is described. This is the theory that complex systems are prone to the occurrence of major accidents. By looking at the recent history of safety incidents in the UK railway industry, it is concluded that the mechanism by which accidents occur in the industry is consistent with organizational accident theory (arguing hypothesis 1).

I then investigate what the theory says about the prevention of accidents, and find that there are three fundamental problems with the application of organizational accident theory to the management of risk in the UK railway industry:

- Lack of safety indicator data.
- Problems with data collection.
- The size and variability of the railway network.

Given these problems, a set of requirements for an ideal risk model are developed to support the management of organizational accidents. These requirements elaborate upon hypothesis 2.

Chapter 4 presents the argument in support of hypothesis 3, that current approaches substantially fail to meet the ideal requirements outlined. The risk modelling approaches used in the UK railway industry are described and then reviewed against the ideal requirements proposed in section 3.7.

In Chapter 5, risk modelling approaches and research which indicate how models that meet the ideal requirements of hypothesis 2 might be developed are reviewed. None of the approaches reviewed fully meet these ideal requirements, however each provides some insight into what a new approach might look like.

In Chapter 6 Bayesian Networks (BNs), and the underlying theory that supports them, are introduced. I then go on to review how BNs have been applied to safety problems and risk analysis, in particular in the aviation industry. This allows ideas for how BN models could be used to build risk models that meet the requirements set out in Chapter 3 to be developed.

The ideas explored in Chapters 5 and 6 are applied in Chapters 7 and 8, where a case study is described which illustrates a new approach to modelling risk in the UK railway industry, based on the development of a parameterised risk model using a BN.

In Chapter 7, the first part of the case study is outlined: the development of a parameterised BN based on the structure of a set of event trees. The case study describes how event trees from an existing railway industry risk analysis can be used to develop a BN model. The model incorporates all logic from the original event tree models and also makes the condition states that form the underlying assumptions of the initial analysis both explicit and variable.

In Chapter 8, Part 2 of the case study, which builds on the work described in Chapter 7, is outlined. A parameterised BN model which incorporates both fault tree and event

tree logic is described. Like the event tree model described in the previous chapter, the model is parameterised by making condition states explicit and variable. The parameterised risk model is quantified using available data and expert judgement. The key features of models of this type are described, and I argue that these features substantially meet three of the five ideal requirements for risk modelling that were previously set out. Therefore this argument partially supports hypothesis 4, that models which meet the ideal requirements set out are possible

In Chapter 9 the argument in support of hypothesis 4 is completed. I argue that the parameterised risk model meets the remaining two ideal requirements that were initially set out in this thesis, namely that it: effectively supports the various stages of a safety management system and; is usable and understandable by those who actually manage safety on the network.

In order to argue that the model meets these requirements, I first describe how such a model would be developed (see section 9.1) and used in practice (see sections 9.2 and 9,3).

In Chapter 10 the argument is summarised and the contribution of this thesis is stated. Further work made possible by the work described here is discussed. Finally, a vision for the future of parmeterised risk models of the type described here is presented.

A glossary of terms is presented in Chapter 11, and the reference list is provided in Chapter 12.

1.6 Published papers

This thesis draws on its author's contributions to seven different published papers.

Section 2.1.3: provides a description of safety decision making principles in the UK railway industry, and their relationship to legal duties that first appeared in (Bearfield 2007b).

The characteristics of ideal risk models presented in section 3.7 and subsequently used to assess various risk modelling approaches were initially proposed in (Bearfield, Dray et al. 2007). This paper also provided some of the review material in sections 4.2.1 and 5.2 and presented the concept of a parameterised risk model that is expanded upon in section 10.4.

Various aspects of the case study described in Chapter 7 have previously been published. The translation from an event tree to a BN described in section 7.1 formed the basis of (Bearfield and Marsh 2005). The development of a BN based on multiple

related event trees described in section 7.4 was first presented in (Marsh and Bearfield 2007a). The case study described in Chapter 7 was published in its entirety in (Marsh and Bearfield 2008).

The use of BNs to parameterise fault trees to allow location specific risk estimates in the railway industry, as described for derailment accidents in sections 8.3 to 8.5, was first explored using an example relating to SPAD accidents in (Marsh and Bearfield 2007b). Section 10.3.1 outlines a proposed approach to the inclusion of organizational indicators in risk models that was initially presented in (Marsh and Bearfield 2004)

2 Risk analysis and modelling principles, definitions and techniques

This chapter presents the essential context required to understand the rest of the thesis. First, concepts relating to risk analysis, risk modelling and safety management and their general application in the UK railway industry are described. A common theme which emerges is a general lack of clarity and consistency in the use of terminology in, and the application of, many of the concepts surrounding risk and safety. Therefore, I state and define the terms that I intend to use in the remainder of this thesis. In particular, the term 'cause' is defined and a number of different categorisations of causal type are proposed.

The modelling and analysis techniques that are commonly used in the railway industry are also described.

2.1 Fundamental principles and requirements

In this subsection, fundamental risk and safety principles and concepts are described and the application of these principles in the UK railway industry is considered, at a high level.

2.1.1 Definition of risk

In a safety context, the term 'risk' is widely understood, in technical and academic fields as well as in general usage, to relate jointly to both the estimated losses which can be caused by a future event and the probability of occurrence of that event. This definition is particularly appropriate for risk in a safety context, as accidents are highly undesirable and (ideally) highly unlikely events.

In the early part of the twentieth century, contrasting views were expressed about the nature of probability, which forms one of the components of risk. Subjectivists like DeFinetti saw probability as purely a product of human belief. Objectivists, like Frank Knight, believed that intrinsically true probabilities did exist and the difficulty lay only in accurately estimating what those probabilities were (Holton 2004). In this thesis, judgement derived probabilities are used. The approach is a subjective one. It accepts that probability estimates can be formed by people's beliefs however it also accepts that objective data might influence people's judgements about probability. Bedford and Cooke point out one consequence of accepting subjective probability in systems engineering:

'Since every rational individual has his own subjective probability it is necessary to find a way of building consensus.' (Bedford and Cooke 2001) p199.

In the fields of safety engineering and safety management, the philosophical issues concerning risk are less important than whether or not it is a useful concept to practically apply to improve safety. The commonly understood definition is therefore considered sufficient. In the UK railway industry's Engineering Safety Management guidelines (RSSB 2007b)[2] risk is defined as 'the likelihood that an accident will happen and the harm that could arise'. Similar definitions may be found in other technical standards used in the railway and other industries (for example (BSI 1999)). These suggest the following equation, which is accepted for risk assessment generally including in the UK railway industry:

Equation 1: $risk = likelihood \times severity$

where 'likelihood' refers to the probability of occurrence of some event in a given period of time, and 'severity' refers to the death or injury that would be caused by this event.

Risks levels are therefore generally expressed in 'fatalities per year' or in similar units incorporating components of time and injury or death. Risk is estimated using expert judgement, available data on the frequency and severity of past events or a combination of the two. Risk can be estimated qualitatively, for example using matrices (BSI 1999; RSSB 2001), or calculated using quantitative techniques like fault and event tree analysis. However, regardless of the technique applied an element of judgement is always required. These techniques are described in section 2.4.

Some have also expressed concerns about the nature of risk. Wilde (Wilde 2001) and Adams (Adams 1995) argue that people, by their very nature, accept certain levels of risk in their lives and that attempts to measure and reduce risk will always be undermined by this mechanism. For example, the driver wearing a seat belt has a tendency to drive faster than the driver who is not wearing one ((Adams 1995), p125).

2.1.2 Legal duty to manage risk

Legal requirements placed on organisations operating in the railway industry mandate some degree of risk assessment. Sections 2, 3 and 4 of Health and Safety at Work Act 1974 (HSWA) (HMSO 1974) require all employers, including railway companies, to manage safety 'so far as is reasonably practicable'. The duty is not just to identify the

---

[2] Commonly known as and hereafter referred to as the 'Yellow Book'.

risks inherent to the company's work activity, but also to effectively minimise them. Companies must minimise all risks that are foreseeable. A company manages risk through the application of its Safety Management System (see section 2.1.4).

2.1.3 Safety decision making

The legal duties that rail companies must discharge in the UK when taking decisions that affect safety are based on a complex mixture of case and statute law. There are, however, few court rulings that help to clarify how the railways can determine what measures are reasonably practicable; thus there is the potential for conflicting views to exist about how to interpret the law. Ultimately, each decision taker is responsible for deciding if the proposed course of action is reasonable, and if necessary, defending that decision in court.

Determination of whether an action is reasonably practicable involves balancing its risks, costs and benefits. The principle was set out in a Court of Appeal judgment in the case of Edwards (Asquith 1949):

'...a computation must be made...in which the quantum of risk is placed on one scale and the sacrifice involved in the measures necessary for averting the risk (whether in money, time or trouble) is placed in the other, and that, if it be shown that there is a gross disproportion between them – the risk being insignificant to the sacrifice - the defendants discharge the onus on them.'

Comparison of the risk associated with an action and its cost, as implied by the Edwards judgement, is not simple as risk and cost are not measured in the same units. In the UK railway industry, risk is generally estimated in Fatalities and Weighted Injuries (FWI) per year.[3] In order to make a comparison of risks with costs, the risk needs to be translated into a financial value. This is done using the industry 'Value of Preventing a Fatality' (VPF), a figure endorsed for use by the Department for Transport, which is currently £1.6 million per statistical fatality averted. This figure was originally developed from studies of what a selection of members of the public said that they would be willing to pay for reduction in risk levels. As the VPF is a measure of what society says they are willing to pay for risk reduction, a sensible and proportionate approach would be to mandate expenditure of resources for the reduction of one FWI only up to the VPF. This would appear logical and reasonable, but it does not sit

---

[3] 1 FWI is equivalent to: 1 fatality; 10 major injuries; 200 reportable minor injuries or; 1000 non reportable minor injuries. (RSSB 2008b), page 27.

comfortably with the judgment in the Edwards case, which requires expenditure to be incurred unless it is 'grossly disproportionate' to the safety benefit. If that judgment is considered to be a true statement of the legal requirements, which is questionable, it offers no guidance to help determine under what circumstances and to what degree additional expenditure might be necessary.

Prior to 2006, when they handed over of their railway responsibilities to the ORR, the HSE and HMRI produced various documents which sought to clarify how they believed the law relating to safety decisions should be interpreted. However, these documents were written from the perspective of the regulator and primarily addressed regulatory concerns. The central purpose of the HSE's document 'Reducing Risks Protecting People' (R2P2) (HSE 2001b) was stated to be:

'opening up [the HSE's] decision making process rather then providing guidance to duty-holders'.

Nevertheless, this document implied that the industry should adopt the principles stated as a means of ensuring that they were taking decisions correctly. In particular it implied that railway companies should take account of loosely defined terms like 'societal concern' in their determination of what is reasonably practicable. Industry found that this guidance was not helpful and only added further confusion. Consultation to address this confusion led to many comments from the industry, typical amongst them being the comment from the Association of Train Operating Companies (ATOC) that it was important that the industry approach to decision taking:

'deliberately excludes any factor relating to subjective perception of risk...ATOC Members do not believe that this concept has any part in a formulation of legal duty' (Bearfield 2007a), page 13.

Following consultation, and in response to the regulatory guidance documents, the industry published 'Taking Safe Decisions' (RSSB 2008b) to clarify its interpretation of its legal duties under HSWA. The industry position is that the determination of reasonable practicability should be taken by a professional person based on the balance between the risk reduction a measure achieves and its cost. The term 'gross disproportion' used in the Edwards judgement is taken to relate to the fact that risk is often very difficult to estimate with accuracy, and the decision taker might tend to err on the side of caution given uncertainty in the risk estimates.

However, both 'Taking Safe Decisions' and ORR guidance (ORR 2008) agree that CBA, and the risk analysis that supports it, do not provide a definitive answer when it comes to the taking of safety related decisions. 'Taking Safe Decisions' states that

'CBA is only an input into the overall decision taking process and is used to inform a judgement.' (RSSB 2008b), page 34.

ORR guidance similarly stresses that:

'CBA cannot form the sole argument in showing that risks are reduced SFAIRP. CBA is not an end in itself, but rather an aid to decision making.' (ORR 2008), page 1.

Because of the uncertainty inherent in the estimation of risk, any decision about reasonable practicability ultimately must be made by an informed professional judgement. In this context, the primary purpose of a risk assessment exercise is to educate and inform decision makers, so that they have a better awareness of the key issues and can make a well-informed judgement. The risk assessment is therefore not seen to be an accurate analysis which gives a definitive answer or option to take forward. There is agreement that there is no substitute for informed professional judgement, although some research has been undertaken to develop models to support the decision taking process itself (Bedford and Quigley 2004).

2.1.4 Management of Safety on the UK railway network

The formerly state owned railway company, British Rail (BR), was privatised in 1994. Prior to this BR's Safety and Standards Directorate (S&SD) undertook safety management tasks for the network as a whole, including accident investigation and audit of all of its five regions[4]. Over the years since privatisation, S&SD evolved into the Rail Safety and Standards Board, which no longer undertakes audit, but which does fulfil a range of other roles in the facilitation and organisation of industry wide safety management activity. For example, RSSB:

- facilitates discussion and agreement between railway companies about how to proceed with industry safety policy decisions.
- maintains a comprehensive model of the risk at the network level to assist with industry policy making and planning (RSSB 2006).
- produces the Strategic Safety Plan (RSSB 2008a), which consolidates the plans of all railway companies operating on the network
- assists industry planning by maintaining Railway Group Standards (RGS) on behalf of the railway industry.

---

[4] The Western, Southern, Scottish, Eastern and London Midland.

- retains a role in facilitating industry monitoring by maintaining the Safety Management Information System (SMIS), which is a database that is used to record monitoring data from the various railway companies. Accident investigation was previously undertaken by RSSB, but is now undertaken by the Rail Accident Investigation Branch (RAIB).

In the UK railway industry, SMSs were previously mandated for railway organisations as part of the Railways (Safety Case) Regulations (HMSO 1994). In April 2006, these regulations were superseded by the Railways and Other Guided Transport Systems (Safety) Regulations 2006 (ROGS) (HMSO 2006), which implement requirements in the Railway Safety Directive (RSD) (EC 2004). These regulations require train operating companies and infrastructure managers to implement a safety management system which must be certified by the Office of Rail Regulation (ORR).

Accident event sequences may cross organizational boundaries. Using the Ladbroke Grove accident (which is reviewed in detail in section 3.3.1) as an example, a SPAD could be partially caused by driver inexperience and partially caused by poor signal sighting. Each of these factors is managed by a separate organisation; therefore a degree of cooperation is required between organisations in order to manage safety effectively. This cooperation might extend to the sharing of risk models, the agreement of common ways of working, or the free flow of safety related information. ROGS places a duty of cooperation on railway companies to work together to manage such risks.

A Safety Management System (SMS) is the name given to the organisation and arrangements put in place by a company to ensure that it operates as safely as is possible. The system must ensure that risks are identified, assessed and effectively controlled. The concept of a SMS is applied throughout all safety critical industries. Different formalisations of this concept exist (for example (CAA 2002; MOD 2004)), however all are based on the same underlying principles. The Health and Safety Executive's safety management guidelines (HSE 1997) provide a clear overview of these principles and the basic contents of a SMS. The guidelines stress that the SMS must consist of the following elements, whose initial letters spell out the acronym POPMAR.

- Policy: a policy stating the general intentions and objectives of the organisation and the criteria and principles upon which it bases its action.
- Organisation: an effective management structure that puts in place the organisation and responsibilities for delivering the policy.

- Planning: clear plans and procedures for the organisation to follow in order to ensure that risks are managed.
- Monitoring: mechanisms for measuring safety performance through the collection of data (active monitoring) and the investigation of incidents and accidents (reactive monitoring).
- Audit: Regular auditing of the organisation to determine how effectively plans and procedures are being implemented.
- Review: Arrangements for the review of the management system itself to ensure that it adapts and evolves with the organisation.

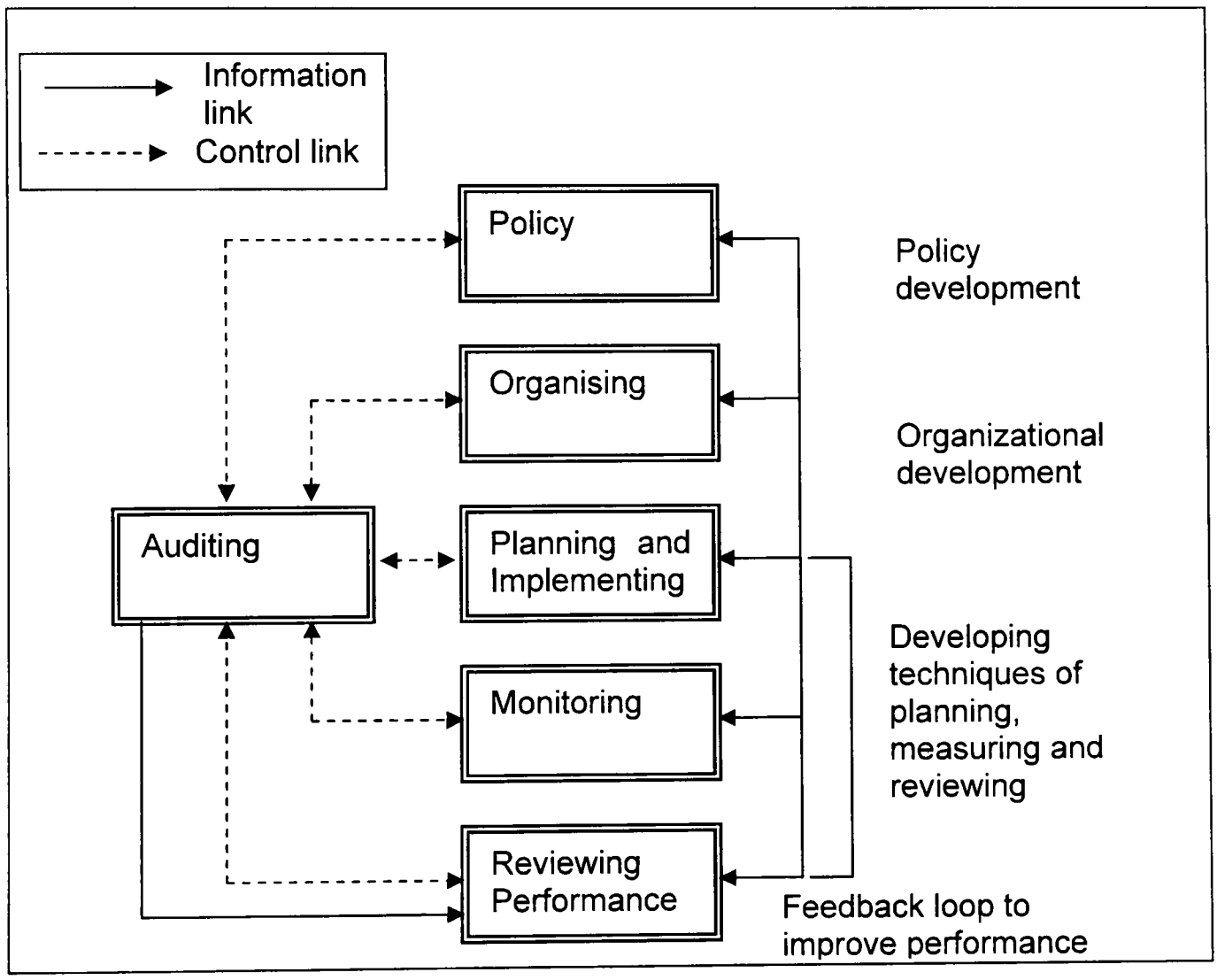


Figure 1: HSE Safety Management System

The relationships between the key elements of a SMS according to the POPMAR guidelines are outlined in the diagram of Figure 1. The diagram shows how information flows between the various SMS elements. A good safety management system is subjected to constant review and update. Work by Kirwan stresses that this is particularly necessary in the modern business environment which is subject to rapid and continual change (Kirwan 2001).

2.2 Risk assessment and modelling terms and concepts

In this section some of the key terms and concepts used for the assessment and modelling of risk are described and the intended use of these terms and concepts within this thesis is clearly outlined.

2.2.1 Accidents

Like many terms in the safety field, 'accident' is regularly used in everyday conversation. The common usage of the term 'accident' and its safety engineering usage are for all practical purpose identical. The Yellow Book offers the definition:

'An unintended event or series of events that results in harm.'

A more precise definition is offered by Leveson, who describes an accident as:

'An undesired and unplanned event that results in a loss (including loss of human life or injury, property damage, environmental pollution, etc).' ((Leveson 2002b), p 265)

This is similar to the definition provided by the Federal Aviation Authority in its system safety handbook (FAA 2000). These definitions do not restrict accidents to events resulting in death or injury. Financial losses and environmental losses are also included. However, as safety management activities are undertaken to reduce health and safety risk, and this is a function of harm to people, these activities therefore focus on a subset of accidents.

Some have taken the definition of an accident further by describing specific types of accident. As already discussed in the last chapter, Reason focuses his concern on *organizational accidents,* a concept that is fundamental to the arguments presented in this thesis:

'These are the comparatively rare, but often catastrophic, events that occur within complex modern technologies...Organizational accidents have multiple causes, involving many different people operating at different levels of their respective companies...organizational accidents...can have devastating effects on uninvolved populations, assets and the environment ((Reason 2002), page 1).

The concept of Organizational Accidents is an evolution of Perrow's concept of Normal Accidents (Perrow 1999). Perrow postulated that there are some major accidents that are inevitable. This is because of the high levels of energy managed by some systems and the complexity of their design. He theorised that it is impossible for human intervention to prevent accidents from occurring in such systems in certain circumstances. Normal accident theory has not influenced safety practice as strongly

as organizational accident theory perhaps because it is much less focussed on the prevention of accidents. Hopkins (Hopkins 1999) provides a critique of normal accident theory that makes this point. In this thesis the concept of a 'normal accident' is not considered helpful. The term *accident* as defined by Leveson is used. Where *organizational accidents* are referred to this alternative term is used explicitly.

2.2.2 Causes

It is self-evident that to prevent accidents from occurring, the various possible accident causes must be known so that they can be prevented from happening. The notion of causality is key to everyday life and in a general sense is universally understood. For example, when we get in our car in the morning and the windscreen is frosted over, we start the car heater to clear it in the knowledge that the frost is *caused* by the cold, and heat will remove it. However rigorous definition and analysis of the concept of causality is much more difficult. There is rarely a single cause of an event. The frost on the car window could equally be considered to have been caused by the moisture in the air. Mathematicians and philosophers, such as John Stuart Mill and Ernest Nagel, have considered issues such as whether a certain set of causes are jointly sufficient to cause an event, and whether all such causes are necessary in order for an event to occur (Ladkin 2002). In recent years, Pearl has sought to provide a rigorous mathematical framework for understanding and interpreting causality (Pearl 2000).

In the railway industry, the term 'cause' is used to encompass a wide variety of different phenomena. Because of this causes are often categorised. The term 'direct cause' (or 'immediate cause') is commonly used to refer to the final event that occurred in the accident event sequence, which should have been prevented by the organisation. Identification of a 'direct cause' is therefore a sequential distinction, and the 'direct cause' may or may not be the focus of subsequent accident prevention activities. This categorisation implies that earlier events, which preceded the direct cause, and which increased the chance that the direct cause would happen, are also causes of the accident. In their report into the Potters Bar accident the Health and Safety Executive describe the 'catastrophic failure in points 2182A' ((HSE 2002c), page 35) as, variously, the initiating, immediate and direct cause of the derailment.

The term 'underlying cause' or 'root cause' is used to refer to the cause that is seen as fundamental to the occurrence of the accident, and without the occurrence of which it is perceived that the accident would not have occurred. Although there are no clear rules to help in the selection of a root cause, this is often done without controversy. As Pearl states:

'Human intuition is extremely keen in detecting and ascertaining [the actual cause].' ((Pearl 2000), page 309).

The 'underlying cause' of the Potters Bar derailment was identified by the HSE as being:

'the poor condition of points 2182A at the time of the incident, and that this resulted from inappropriate adjustment and from insufficient maintenance compared to what was necessary for their operating environment and safety functions.' ((HSE 2002c) page 37).

Note that according to this interpretation causes are not always events. The root cause of the Potters Bar derailment was 'the poor condition of points 2182A'. Accident reports often list many 'conditions' as contributory to the occurrence of an accident. These conditions are sometimes referred to as influences, influencing factors or just factors. In this thesis, the terms 'root cause' and 'direct cause' (or their variants) are not used. Both events and conditions are considered to be 'causes', provided that their occurrence or state respectively result in an increase in the likelihood of occurrence of an accident. In section 2.3, types of event and condition are categorised, and therefore by extension so are types of accident cause.

2.2.3 Hazard

The Railway Safety Standards 50126-50129 (BSI 1999; BSI 2001; BSI 2003) and the international standard IEC61508 (BSI 2002) define a hazard as 'a physical situation with a potential for human injury.' In order to understand and apply the concept of a hazard usefully in the safety field systems engineering concepts are applied.

A hazard is expressed at the boundary of a system. For example if we are introducing a new type of colour light signal onto the railway network, we are concerned with its interfaces to the wider railway system. Hazards would therefore relate to: possible misinterpretation of the signal by train drivers; the interfacing of the signal to the signal interlocking computer; the interfacing of the signal to the lineside railway power supply and so on.

Figure 2 (taken from the Yellow Book (RSSB 2007b), page 152) illustrates the concept of the system boundary and shows how the hazard should be specified at that boundary. A hazard is useful in safety engineering as it provides a focal point for any analysis. Causes of hazards are potentially under the control of the organisation responsible for the system. In the case of our colour light system these causes would

include component failures that result in the operating parameters of the signal falling outside of its specification.

Causal analysis, such as fault tree analysis (see section 2.4.2), is used to understand these effects. For those who interface externally with the system, the hazard also provides a focal point, as they need to be aware of the nature of the potential hazard and how they could prevent the hazard escalating into an accident. The diagram highlights that once a hazard exists then it is possible that an accident will occur.

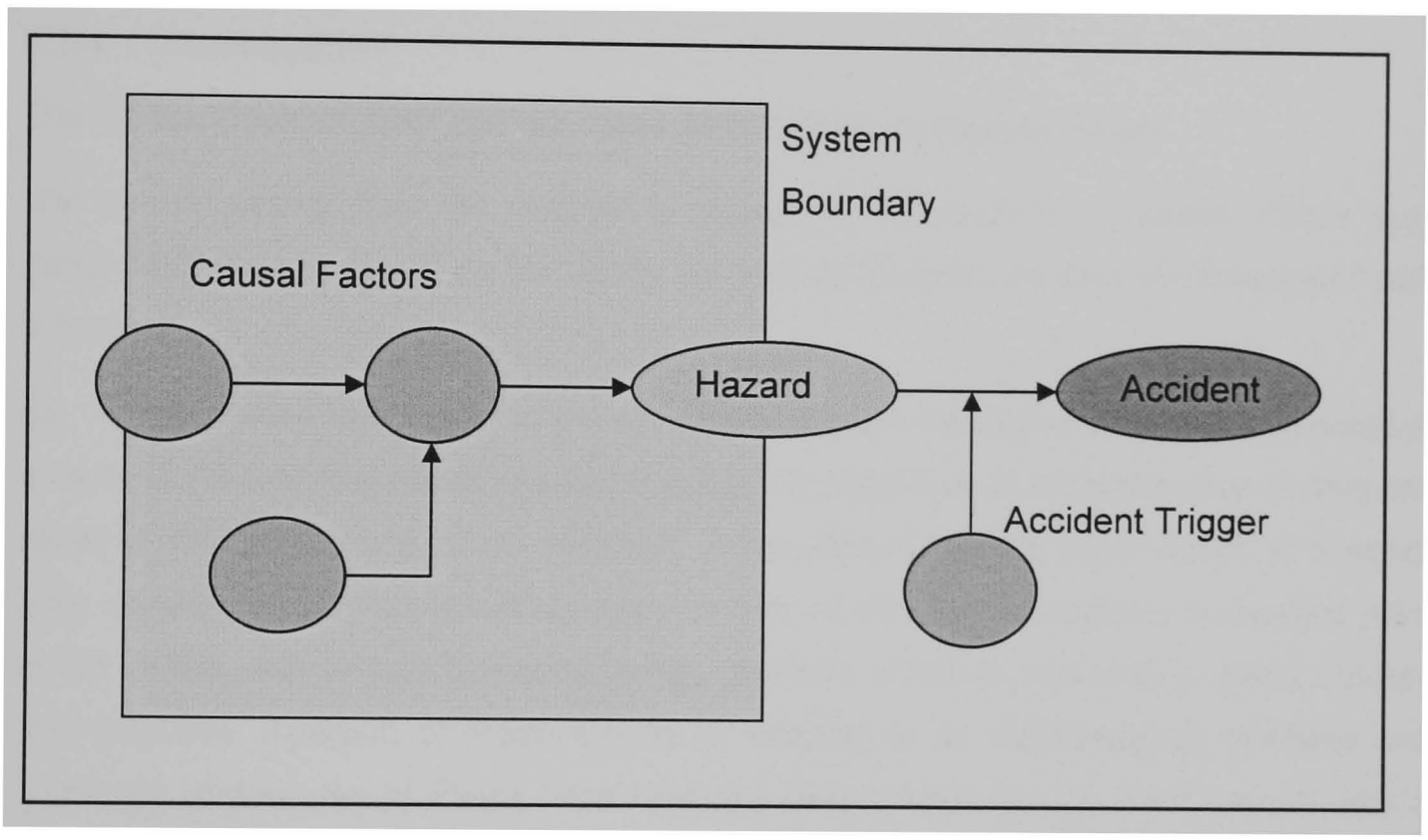


Figure 2: Safety analysis system boundary

The Yellow Book states that:

'Any change to the railway can be regarded as introducing a new system, or changing an existing one. Understanding the boundary between a system and its environment is a prerequisite to understanding how the system might contribute to an accident (that is understanding what its hazards are).' ((RSSB 2007b), page 27).

The yellow book is concerned with engineering change, and hence its focus is on the introduction of new systems to the railway. However the operational railway network as a whole is also a system and the same concepts apply. This system incorporates both the train and the track and all other elements of the operational railway. The presence of an undetected track fault could be considered to be a hazard expressed at the boundary of this larger system. Once this hazard has occurred it is a matter of circumstance whether or not a derailment occurs. If a train is permitted to traverse that

section of track, a derailment accident might occur, and there are no further measures under the control of the railway industry that could prevent it.

The identification of hazards is the first stage in any analysis of modelling of risks. To identify hazards, a safety engineer generally gathers together a group of domain experts and takes them through a structured process such as the use of checklists of the types of hazards and accidents that might occur. The concept of a hazard is fundamental to the risk modelling work subsequently described in this thesis.

2.2.4 Consequence

The Yellow Book ((RSSB 2007b). Page 229) defines consequence as:

'the results arising from the addition of energy or exposure to a hazard. These may range from benign results to accidents. Several consequences may be associated with a hazard'

As , in the safety field the term 'consequence' is often closely related to the concept of a hazard. As was described in section 2.2.3, the presence of a hazard may or may not result in the occurrence of an accident. A derailment hazard could result in a minor train derailment with no resulting injury or loss of life, or alternatively a derailed train could collide with a train travelling in the opposite direction resulting in many injuries and fatalities. Analysis of these events is referred to as consequence analysis and generally makes use of Event Tree Analysis (see section 2.4.3). Each hazard has a range of possible consequences. To understand risk and manage safety we are concerned with a subset of these consequences, the ones resulting in injuries and fatalities to people.

2.3 Types of cause

In section 2.2.2, the concept of a cause was described and it was concluded that causes could be either events or conditions. In this section, events and conditions are further distinguished by considering sub-categories of each. Categorisation of events into failures, human errors and external events is proposed, along with categorisation of conditions into technical, operational, organizational and performance conditions. Figure 3 shows this hierarchy of different types of cause. The different casual types are then described.

2.3.1 Events

Understanding and rigorous definition of the conceptual meaning of the term 'event' is closely related to understanding and definition of 'cause'. The definition of the term is similarly an unresolved and complex philosophical question which has been the subject of debate by philosophers like Kim (Kim 1973; Kim 1977) for many years. For our purposes it is sufficient to define an event as an occurrence that happens instantaneously or over a short period of time. An event can be reasonably approximated as having only two states: 'event has occurred' and 'event has not occurred'. The two-state approximation simplifies the modelling of events, for example by making them suitable for modelling in a fault tree (see 2.4.1).

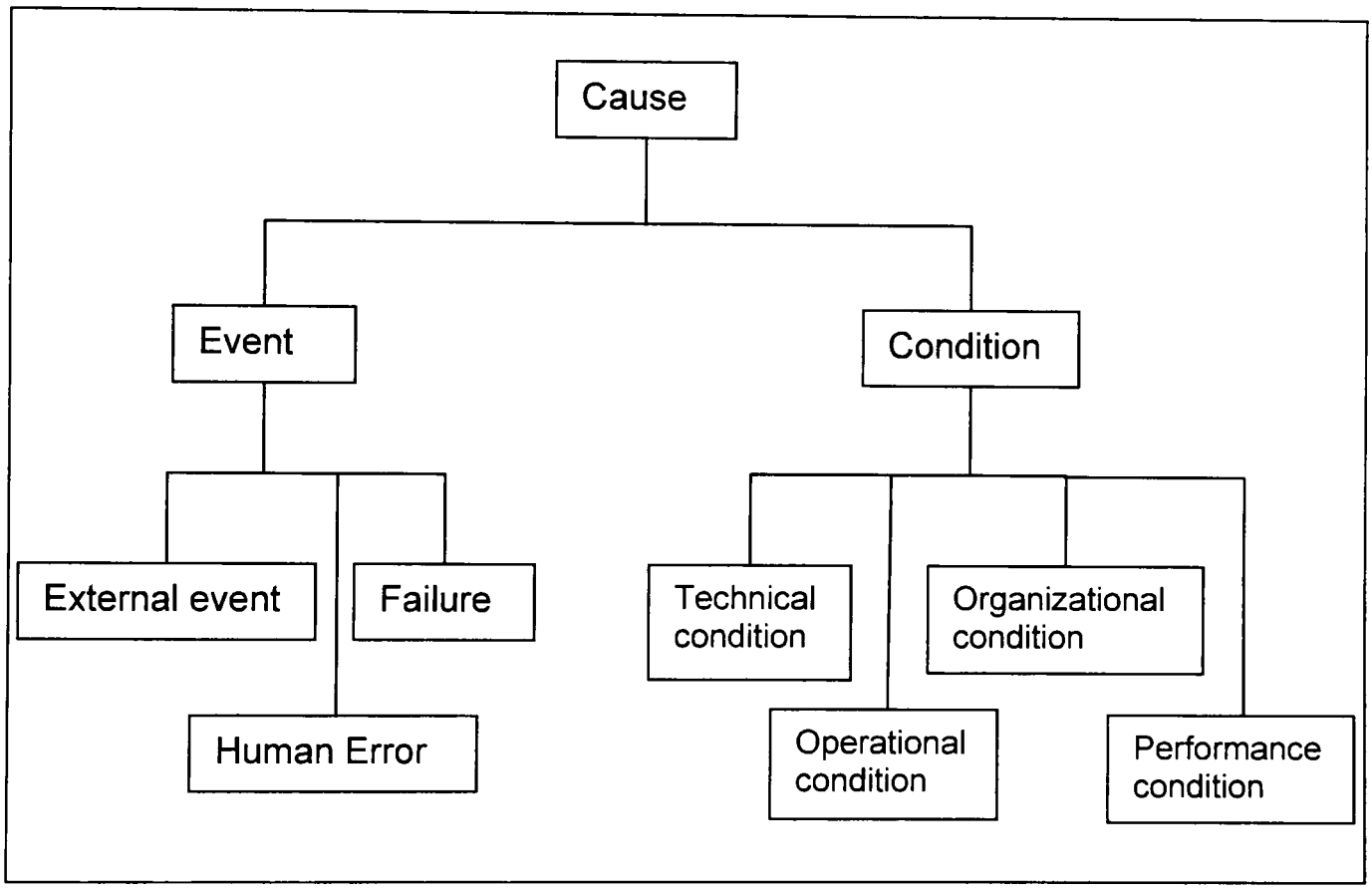


Figure 3: Hierarchy of causal types

2.3.1.1 Failures

Smith defines a failure as:

'Non-performance to some defined performance criteria'. ((Smith 1997), page 11)

The concept has found use widely in the field of reliability engineering which developed in the aftermath of the Second World War, and was initially developed to support the analysis of the Minuteman launch control system (Watson 1961). To design high reliability systems, designers need to be aware of how the individual components of these systems could fail. Using this information, they can determine how the system itself might fail and hence improve on its design, often by building redundancy into the

system. The concept developed for application to electrical/electronic systems, mechanical systems and their hybrids. Failure rates for electrical/electronic and mechanical components can be derived from manufacturer's data. Components are tested by manufacturers over a period of time, and the average failure rates under a range of operating conditions are taken to be indicative of the failure rate of components of the same type. US military specifications are also available which provide guidance on calculating the failure rate of electronic components using their operating parameters (DoD 1991). It has been argued that the prediction of failure rates is complex and often inaccurate (Blanks 1998). However, there are some characteristics of failure rates that make them easier to quantify than human error rates (see section 2.3.1.2). The performance of hardware is less susceptible to external influences than people are and it is possible to control the environment to limit the effect of these influences. For example, solid state electronic components are specified given certain power dissipations, and certain operational temperature ranges. These conditions can be controlled, and therefore the failure rates of these components made more predictable.

Failure of electrical, electronic and mechanical components is often practically instantaneous, and these failures, for example the open circuit failure of a resistor inside a colour light signal or the fracturing of a rail as a train passes over it, can therefore be considered to be events.

2.3.1.2 Human error

As the reliability of man-made systems has improved, the relative importance of the human contribution to safety performance has risen. Research into human error, and how to prevent it, has a long history and in the latter years of the twentieth century coherent frameworks for understanding and managing human error emerged, such as Reason's Generic Error Modelling System (GEMS) (Reason 1990) and the skill-rule-knowledge framework (Rasmussen and Jensen 1974) from which it is derived.

A good example of a human error in the railway industry is the occurrence of a Signal Passed at Danger (SPAD). A SPAD is an unintentional violation of a safety procedure by a driver. Edkins and Pollock concluded that SPADs are skill based errors which occur because of the repetitive nature of train driving tasks, and loss of attention that inevitably occurs as a result (Edkins and Pollock 1997). Significant work has been undertaken into the mechanisms by which SPADs occur over many years, for example: (Buck 1963; Williams 1977; Van-der-Flier and Schoonman 1988; Wright 2000; Wright and Embrey 2000; Wright, Embrey et al. 2000). Much of the work in this area is

concerned with classifying and understanding different error types and the circumstances in which they can occur.

The rates of occurrence of human errors in different circumstances can be estimated. One of the most popular techniques for estimating human error rates is the Human Error Assessment & Reduction Technique (HEART) (Williams 1986). The technique provides a set of generic task types with associated error probabilities. Activities to be undertaken are matched to the list of generic tasks, and hence to their associated probabilities. A further list of error producing conditions is provided and these are used to scale the generic probabilities in accordance with the specific sets of conditions. The failure rates and factors are derived from an in depth survey of literature and incident reports.

Estimating human failure rates in this way depends to a great extent on the application knowledge of the analyst and their skill at applying the particular technique. A validation exercise of three human reliability quantification techniques, including HEART (Kiwan 1996; Kirwan, Kennedy et al. 1997) found that only 38% of the 30 human error probabilities analysed were within a factor of three of values obtained experimentally. It is harder to control the influences that may affect human failure rates. The HEART technique asserts that these rates are influenced by a wide range of 'error producing conditions'. It is not always possible to manage the environment that people operate in to constrain all of these conditions or completely control the environment that people operate in and this complicates the estimation of human error rates. Nevertheless these techniques are widely used for safety analysis.

2.3.1.3 External event

The occurrence of some events increases risk, although the events could not in themselves be considered failures or errors. For example, if two trains pass each other on adjacent tracks, this is for the most part an unremarkable event. However, if one derails this event has much more significance and indicates the presence of much increased levels of risk. In this thesis these types of events are defined as 'external events'. They are a matter of circumstance and are generally events occurring outside the system boundary shown in Figure 2.

2.3.2 Conditions

In this thesis a condition is defined as the particular state of a person or thing at a given point in time. The condition may be in a stable state, it may change gradually over time, or it may be in a constant state of change. As with the definition of an event, this is not

a rigorous definition, and therefore we must use our judgement and intuition when applying either concept. Unlike events, conditions are often not well approximated as Boolean variables as their states are often best measured or conceptualised as continuous values.

The condition of the rail that fractured under the train at Hatfield (see section 3.2.3) evolved. When initially installed, its condition was good. However, over time, due to the effects of trains passing over it, it began to exhibit symptoms of gauge corner cracking. Just prior to its fracture, its condition could be considered to be poor. Conditions can affect the likelihood of occurrence of events in an accident sequence, but they do not definitely determine whether or not events, and ultimately accidents, occur. All conditions could be unfavourable, and yet an accident might not have occurred. The poor condition of the rail made the event 'rail fracture occurs' much more likely. Yet there were other locations on the network with worn rail, at which accidents did not occur. In organizational accident theory, Reason talks about 'latent conditions' ((Reason 2002) page 10) and gives a diverse set of examples such as:

'poor design, gaps in supervision, undetected manufacturing defects or maintenance failures, unworkable procedures, clumsy automation, shortfalls in training, less than adequate tools and equipment'.

The categorisation of conditions proposed is similar to Reason's categorisation of 'local workplace factors' and 'organizational factors' although according to the definition used here the former describes both technical and operational conditions. 'Performance conditions' are considered as an additional condition type.

2.3.2.1 Technical condition

The state of the railway's various items of physical infrastructure are categorised as 'technical conditions'. Technical conditions have featured as causes in all of the major UK railway accidents that were highlighted in section 3.2. According to the categorisation of causes used in this thesis categorisation the condition of the rail prior to the Hatfield accident was a 'technical condition' which was considered to be the 'root cause' of the accident. Prior to the Ladbroke Grove accident the condition of the signalling infrastructure, in particular the difficulty in sighting the signal that was passed at danger, was an identified cause of the accident. Evidence taken at the inquiry stated:

'The general signal viewing conditions in the Paddington area present the drivers with an exceptionally difficult signal reading task. The complexity of the layout and signal gantries, the range of approaches, and the obscuration of signal aspects by overhead

line equipment presents most difficult visual and interpretative challenges to drivers'. ((Cullen 2000) page 55).

In the Potters Bar accident, the HSE concluded that they were:

'satisfied that an explanation can be given for the failure of points 2182A based on evidence of the poor condition of these points to an extent that they were not "fit for purpose" for the operating environment and safety related functions expected of them.' ((HSE 2002c) page iv).

2.3.2.2 Operational condition

The factors that affect the performance of front line staff undertaking safety related duties are categorised here as 'operational conditions'. In section 2.3.1.2 it was described how error producing conditions are used to determine human error rates. According to the categorisation used in this thesis these conditions are all 'operational conditions'. In the rail specific technique they include 'time availability', 'high workload' and 'fatigue'.

Section 3.3.1 will go on to describe operational conditions that were known to be relevant to the occurrence of the train accident at Ladbroke Grove, such as the signaller responsible for the track on which the accident occurred was found to be operating under demanding time constraints.

2.3.2.3 Organizational condition

Where organisations fail in their duty to prevent accidents, it is usually in the structuring of the organisation, the effectiveness with which it works, and the culture of the organisation. The term Safety Culture was developed by INSAG in the wake of the Chernobyl nuclear accident to capture some of these concepts (INSAG 1991). INSAG defined safety culture as:

'that assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, nuclear plant safety issues receive the attention warranted by their significance.'

INSAG argues that safety culture is dependent on personal attitudes, habits and other intangibles. However, such qualities lead to tangible manifestations that can be used to test and monitor the safety culture of an organisation. In this thesis, failings or inefficiencies in an organisation, which have an effect on the likelihood or severity of accidents are categorised as 'organizational conditions'. 'Organizational' conditions relate to the performance of an organisation or its components and the setting of these

condition states for a particular analysis is qualitative and a matter of judgement. These conditions are not set, but emerge from the organisation. 'Organizational' conditions cannot be directly measured, but their state can be correlated to other indicators. For example, the priority that a senior manager of a company gives to safety cannot be directly measured, but the time that this manager spends on company walkabouts and direct discussion with his employees about safety matters could be.

The report into the Ladbroke Grove accident acknowledged that such conditions were implicated in the occurrence of the accident. One example given was the inability of the discussions of a group convened to investigate the risk of SPADs at Ladbroke Grove, prior to the accident, to agree on any significant actions to improve signal sighting. Railtrack admitted that:

'There were probably too many groups and their functions overlapped. While a number of good ideas were formulated and debated there was a lack of a single person or body to ensure that prompt and appropriate action was taken. The organisation, in this respect, was diffuse.' ((Cullen 2000) page 135).

The Cullen report goes on to conclude that this ineffectiveness was a symptom of poor safety culture. Another example of poor organizational performance was in the approach to driver recruitment applied by the train operator, Thames trains. Lord Cullen states:

'It is not suggested that Mr Hodder was in any way unsatisfactory as an applicant. However the fact that Thames Trains were prepared to bypass their own procedures, due to the need to recruit drivers quickly because of an increase in traffic, suggests that they had set a production requirement ahead of following procedures appropriately.'

The organization appears to have performed its recruitment role poorly. This organizational condition is something that might have been able to be identified by an auditor or through safety culture assessment.

2.3.2.4 Performance conditions

Performance conditions are conceptually different from the three other types of condition outlined. They do not relate to any particular weakness of the system. A good example of a performance condition is train speed. A train might be travelling at a speed of 10mph or it might be travelling at 100mph. In neither case would train speed be considered to be 'poor'. However, the speed of the train is a fundamental consideration when estimating risk. It is the movement of the train that creates the risk and train speed is one of the key determinants of the severity of the accident. Another

example of a performance condition is traffic density. Sometimes the track is busy, sometimes it is not. However, when it is busy the probability of trains colliding with each other is increased. To estimate risk in any given situation a clear understanding of the state of performance conditions is needed. 'Performance conditions' is also considered to include elements of organizational planning such as the intervals between technical inspections.

2.4 Commonly used modelling and analysis techniques

The key terms and concepts that must be understood in order to assess and analyse risk and use this information to manage it have now been defined. Next the techniques that are most commonly used in the UK railway industry to model and estimate risk are described, namely:

- Risk Matrices
- Fault Tree Analysis
- Event Tree Analysis
- Bow-tie models

2.4.1 Risk Matrices

Risk matrices are used as a quick and relatively simple way of assessing the risks to which a project or company is exposed. The approach is strongly supported by the use of expert judgement. First, the boundary of the system under analysis is defined and all of the hazards identified. Each hazard is then assigned an estimated likelihood of occurrence and severity rating according to a set of predefined categories. These categories are then combined to form an overall risk ranking, as indicated by a risk ranking table that crudely apples the risk equation shown in 2.1.1. The risk matrix approach is commonly used in a range of industries and is embedded in standards like BS EN51026 (BSI 1999) or the military standard 00-56 (MOD 2004). In the UK railway industry, the railway group guidance note GE/GN8561 (RSSB 2001) suggests a particular approach for train operators to use to analyse all of the risks that they need to manage through the application of their safety management system. Table 1 and Table 2 show the ranking approach proposed. Note that both tables use the terms 'frequency' and 'consequence' rather than the terms 'likelihood' and 'severity' which are used in BS EN50126. In this context the equivalent terms should be taken to mean the same thing.

The advantage of the risk ranking approach is that it allows an analyst to assess the risk from a large number of hazards quickly. However, the methodology does not enforce or rely upon any analysis of the causes of hazards and accidents and no model of cause and effect is produced. Therefore, no detailed record of the assumptions under which risk is estimated is required, although a diligent analyst would record key assumptions.

Frequency		**Consequence**	
A	Rare – e.g. 1 in 50 years	A	Negligible – e.g. slight injury, no absence from work
B	Infrequent – e.g. 1 in 10 years	B	Low – e.g. requiring first aid treatment
C	Occasional – e.g. 1 per year	C	Moderate – e.g. injury leading to lost time accident
D	Frequent – e.g. 1 per month	D	High – e.g. single fatality
E	Regular – e.g. 1 per day	E	Severe – e.g. multiple fatalities

Table 1 Example qualitative ranking scheme

	Consequence				
Frequency	A	B	C	D	E
E	M	M	H	H	H
D	L	M	M	H	H
C	L	L	M	M	H
B	L	L	L	M	M
A	L	L	L	L	M

Table 2 Qualitative Risk Categories (L = low, M = medium, H = High)

Essentially the ranking relies on the shared mental model of the gathered experts. This mental model may be flawed, and cannot subsequently be reviewed or audited. Because of these weaknesses, ranking approaches are often used to filter out the hazards with the highest estimated risk rather than as the primary means of risk analysis. Further analysis of these hazards would then be undertaken in more depth, using techniques such as fault and event tree analysis, which are described in the following sub-sections.

2.4.2 Fault tree analysis

Smith describes a fault tree as:

'A graphical method of describing the combinations of events leading to a defined system failure'. ((Smith 1997), page103).

The system failure being analysed is called the 'top-event', and the individual events are called 'base events'. The basic fault tree uses AND and OR gates to link the base events to the top event. Other types of gate can be used to model more complex logical conditions, for example exclusive OR gates, or NOR gates. The symbols for AND gates, OR gates and base events are shown in Figure 4. The event conditions that input to the gates can be considered to be either logically true or false only. Base events represent the limit of resolution of the fault tree.

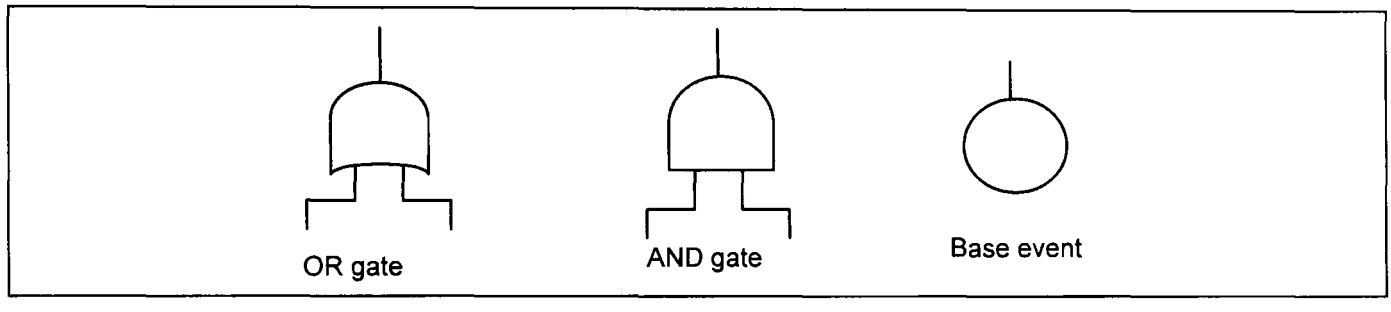


Figure 4: Fault tree Or gate, AND gate and base event

A cut set is a group of base events whose simultaneous occurrence causes the top-event to occur, and a minimal cut set is the cut set group comprising the least number of base events. AND and OR gates in fault trees each equate to a single Boolean algebraic expression. A fault tree can therefore be described as a list of logical statements and these logical statements can be simplified using Boolean reduction techniques. The resulting simplification describes the top-event in terms of a finite number of minimal cut-sets. Calculation of top event probabilities is automated using computer programmes such as (Isograph 2007).

Fault Trees are used across a variety of industries and there is extensive guidance available in how to construct and use them (for example (IEC 1990) and (Vesely, Goldberg et al. 1981)). They were developed, and have found substantial use, as a tool to support analysis of the reliability of hardware systems, a use for which they are well suited. The diagram of Figure 5 (from (Smith 1997), page 104) shows a classic fault tree analysis undertaken to determine the reliability of a fire protection water deluge system. All of the base events are failures of technical components or systems. As was discussed in section 2.3.1.1 these failures are usually approximated well by the bivalent two-state conceptualisation enforced by the use of fault trees. There are also established methods of calculating the failure rates of electrical and mechanical components.

The fault tree shows where different combinations of base events ultimately have the same system effect. The top event describes this system effect, and the fault tree shows how it could arise from the occurrence of different base events, individually or in combination.

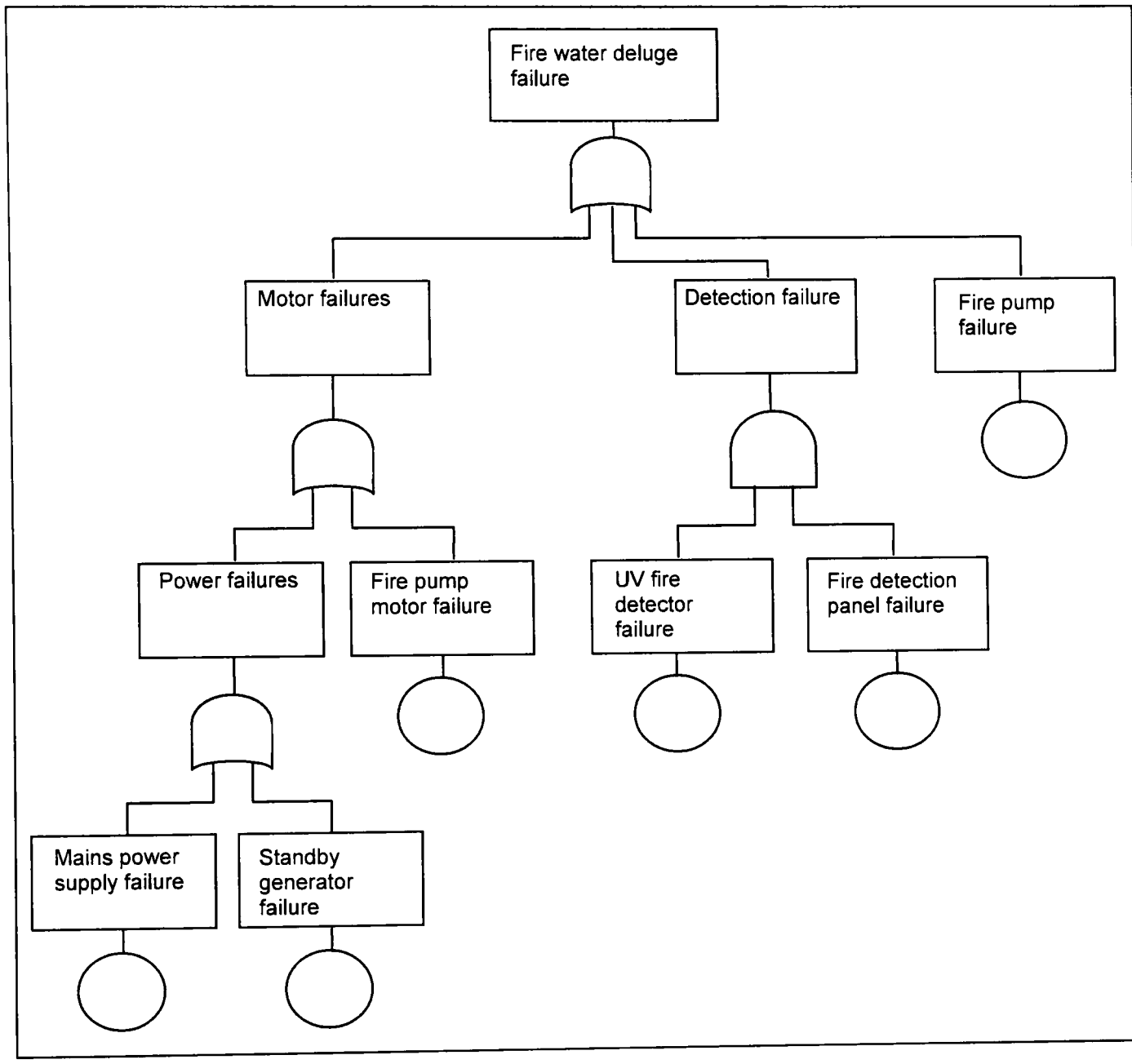


Figure 5: Fault tree for a fire protection water deluge system

Separately modelled fault tree base events are considered to be independent events. Any common cause between base events must be explicitly modelled. There are various techniques for doing this. For example the same base event might be repeated in different parts of the model thereby assuming that both events always have the same Boolean state. Correlations between base events can be modelled in fault trees using a beta factor to represent a percentage of base event failures that lead to the common cause failure of one or more other base events.

Fault trees are used in safety analysis as well as in reliability analysis. When used in safety analysis the top event of the fault tree is a hazard. Whereas analysis of the reliability of systems focuses on the failure of hardware components, safety analysis

will tend to involve human errors in addition to failures as safety assurance usually has a human element. The diagram of Figure 6 shows a fault tree developed for safety analysis in the UK railway industry (Campbell and Kennedy 2003). The top-event is the occurrence of uncontrolled 'gauge spread'. Gauge spreading occurs when railway lines separate such that the distance between them is no longer within acceptable tolerances, given the distance between the wheels of trains passing over that section. Gauge spreading is a hazard as its occurrence could derail a passing train.

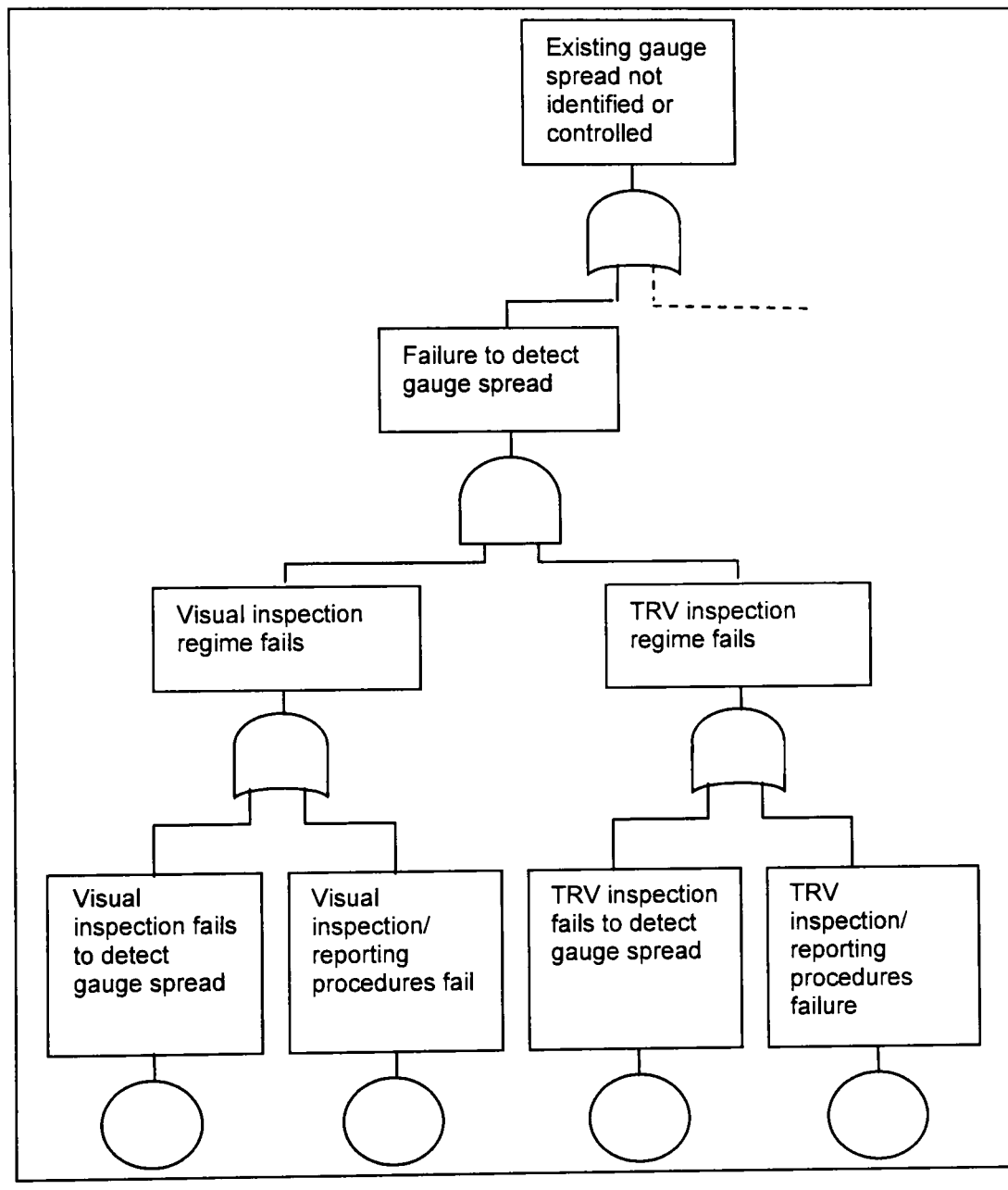


Figure 6: Human Error modelled in a fault tree

The fact that safety analysis using fault trees often involves human error rate quantification creates different problems for the analyst when compared with their use for reliability analysis. In the fault tree of Figure 6, although the base event descriptions are not clear, on close inspection it can be seen that all base events involve some degree of human error. For example 'Visual inspection fails to detect gauge spread' might be more clearly described as the human error 'inspector fails to notice gauge spread'. The probability of occurrence of this event would tend to depend on a range of

factors such as the competence of the inspector, their fitness for duty, and whether or not there were any distractions present at the time the event occurred 'Visual inspection/reporting procedures fail' represents a failure of the system of work rather than a specific human error, however the causes of this event are likely to be procedural failures caused by a human error.

Often when analysts define human errors in fault trees they do not rigorously describe them as events, and this undermines the use of the method, as the conceptual clarity provided by the method is lost. Another difficulty is that the estimation of human error rates is less well established than the estimation of component failure rates, and can be a more difficult process (see section 2.3.1.2). Many error-producing conditions are needed to provide human reliability estimates, and the state of these conditions can vary widely from situation to situation. The conditions relating to a particular analysis therefore form the underlying assumptions of the analysis however they are often not documented. For example, the error producing conditions relevant to the estimation of a probability of occurrence of the human errors modelled were not described in the report from which the fault tree of Figure 6 is taken.

2.4.3 Event Tree Analysis

Event trees model the possible sequences of events between an initiating event and its consequences. When used in safety analysis the initiating event is generally a hazard. Figure 7 shows a simple event tree for the initiating event of a signal passed at danger (SPAD) occurring on the railway network. The branches of the tree are determined by answers to situational questions posed at the top of the diagram. Responses to these questions do not have to be simply 'success' or 'failure'. A number of responses can be represented at each stage as long as:

- each of the responses to a given question in a particular branch represents a discrete system state i.e. the states are mutually exclusive, and
- the probability of all such states sums to one i.e. the states at each branch are exhaustive.

However in practice a Boolean, two-state approach (true, false) is most often used. The probabilities of occurrence of each of the consequences shown on the right-hand side of the diagram can be calculated simply by multiplying the probabilities of each of the event outcomes on the branch leading to that consequence.

For example the probability (P) of a 'high speed collision', given that a SPAD has occurred is:

$$P = 0.1 * 0.1 * 0.5$$
$$= 0.005$$

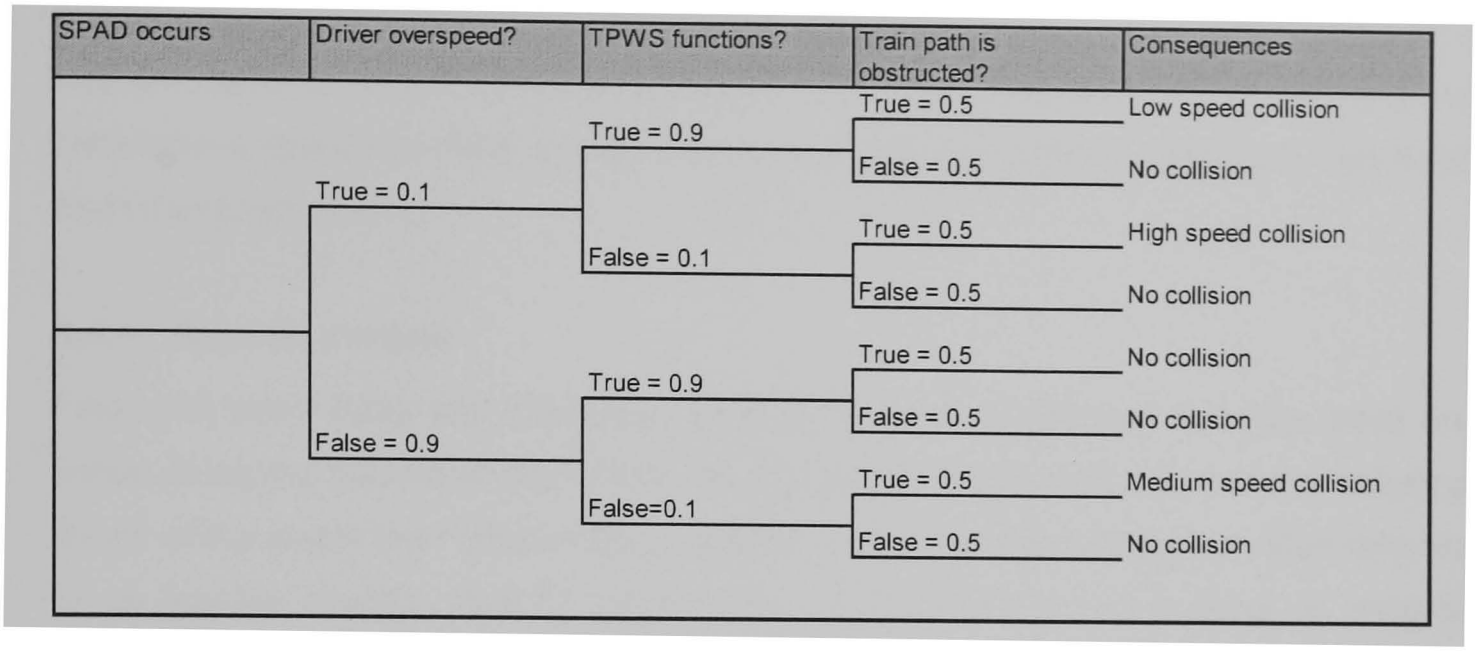


Figure 7: Indicative event tree modelling the consequences of a SPAD

In order to calculate the estimated likelihood of occurrence of the high-speed collision this value should be multiplied by the likelihood of occurrence of the initiating event, the SPAD. This probability could be obtained using fault tree analysis or a similar technique. As was stated in section 2.1.1:

*Risk = likelihood * severity*

Using the information in the event tree, if the probability of occurrence of the initiating event is known, it is possible to estimate the risk associated with this hazard. The event tree analysis describes the range of outcomes that are considered possible given the occurrence of the initiating event. The severity associated with each of the defined event tree consequences is calculated separately using whatever methods may be appropriate. For example, from existing data, or an analysis of crashworthiness of rolling stock, it might be estimated that a high speed collision would result in approximately 10 fatalities. Having estimated the severity of each consequence the corresponding risk is calculated simply by multiplying the estimated likelihood of each consequence with its severity. The total risk associated with the initiating event is calculated by summing the risk associated with each consequence.

An analyst must be aware of potential conditional probability effects when deriving probability estimates for an event tree. For example, with the tree of Figure 7 the probabilities assigned for 'TPWS functions' may be affected by consideration of whether or not the driver is overspeeding. The TPWS may be less likely to trigger when the train passes over it at excessive speed. The question to ask is therefore 'how likely

is it that TPWS will function given that the train is overspeeding?' In the example shown the implicit assumption is that the speed of the train has no significant effect on the functioning of TPWS, as the probabilities in the upper and lower halves of the event tree are identical. Event trees can be built using simple spreadsheets to automate the calculations described here or with specially developed software packages like Fault tree+ (Isograph 2007).

2.4.4 Bow-tie models

Fault and event trees are often used together in order to estimate risk. The trees are linked using the hazard which is both the 'top-event' of the fault tree and the 'initiating event' of the event tree. When linked together in this way the models are often referred to as bow-tie models. Bow-tie models have been used for many years to analyse hazardous systems, in particular in the oil and gas industry (HSE 2006).

In a bow-tie model the failures leading to the accident are analysed in the fault tree part of the model. The events that occur following the hazard are analysed in the event tree, on the right of the model. The bow-tie structure assumes that these events are independent. However, since both the occurrence of the failure and the evolution of the accident may be influenced by the same conditions in the environment of the system, correlations between events in each model can easily occur.

In the Yellow Book the use of cause-consequence models is suggested for risk analysis rather than the use of fault and event trees. The causal part of these diagrams consists of fault trees. Consequence analysis is undertaken using a technique identical to event tree analysis, with the exception that paths do not always branch at event outcome points. Instead where consequences are identical, paths converge. This reduces the number of separately modelled consequences associated with some hazards. However, this is a minor difference and for all practical purposes cause-consequence diagrams can be considered identical to bow-tie models.

2.5 Chapter summary

In this chapter, the concepts that underpin risk modelling and assessment in the UK railway industry were defined. Definitions were provided for key concepts that will be used throughout this thesis. In particular, causes of accidents were defined as being of two types: events and conditions. A sub-categorisation of each of these types of cause was also provided.

3 Managing Organizational accidents in the UK railway industry

In this chapter, organizational accident theory, the theory that complex systems are prone to the occurrence of major accidents, is described. By looking at the recent history of safety incidents in the UK railway industry it is concluded that the mechanism by which accidents occur in the industry is consistent with organizational accident theory (arguing hypothesis 1).

What the theory says about the prevention of accidents is then investigated. This investigation finds that there are three fundamental problems with the application of organizational accident theory to the management of risk in the UK railway industry:

- Lack of safety indicator data
- Problems with data collection
- The size and variability of the railway network

Given these problems, a set of requirements for an ideal risk model to support the management of organizational accidents are proposed. These requirements elaborate upon hypothesis 2.

3.1 Organizational accident theory

(Reason 2002) explains that, in safety critical industries multiple, sometimes redundant, defences are put in place to ensure safety. These can be:

- implemented in engineered systems.
- undertaken by people following procedures or
- provided by the wider management processes of an organisation.

He refers to these various measures as 'defences in depth'. According to Reason, organisations in which accidents are prevented by 'defences in depth' are susceptible to 'organizational accidents'. These accidents occur as the result of multiple failures occurring to all safety controls. The accident would not be caused by any one of these failures or errors individually but their coincident occurrence leads to catastrophic consequences. 'Organizational accidents' occur because of a fundamental contradiction: as catastrophic accidents are undesirable many different types of defences are put in place to protect against them; however this creates complexity which is hard to manage and therefore increases the chances that all defences may be

simultaneously breached. Reason uses the 'Swiss-cheese model' to illustrate the mechanism by which 'organizational accidents' occur.

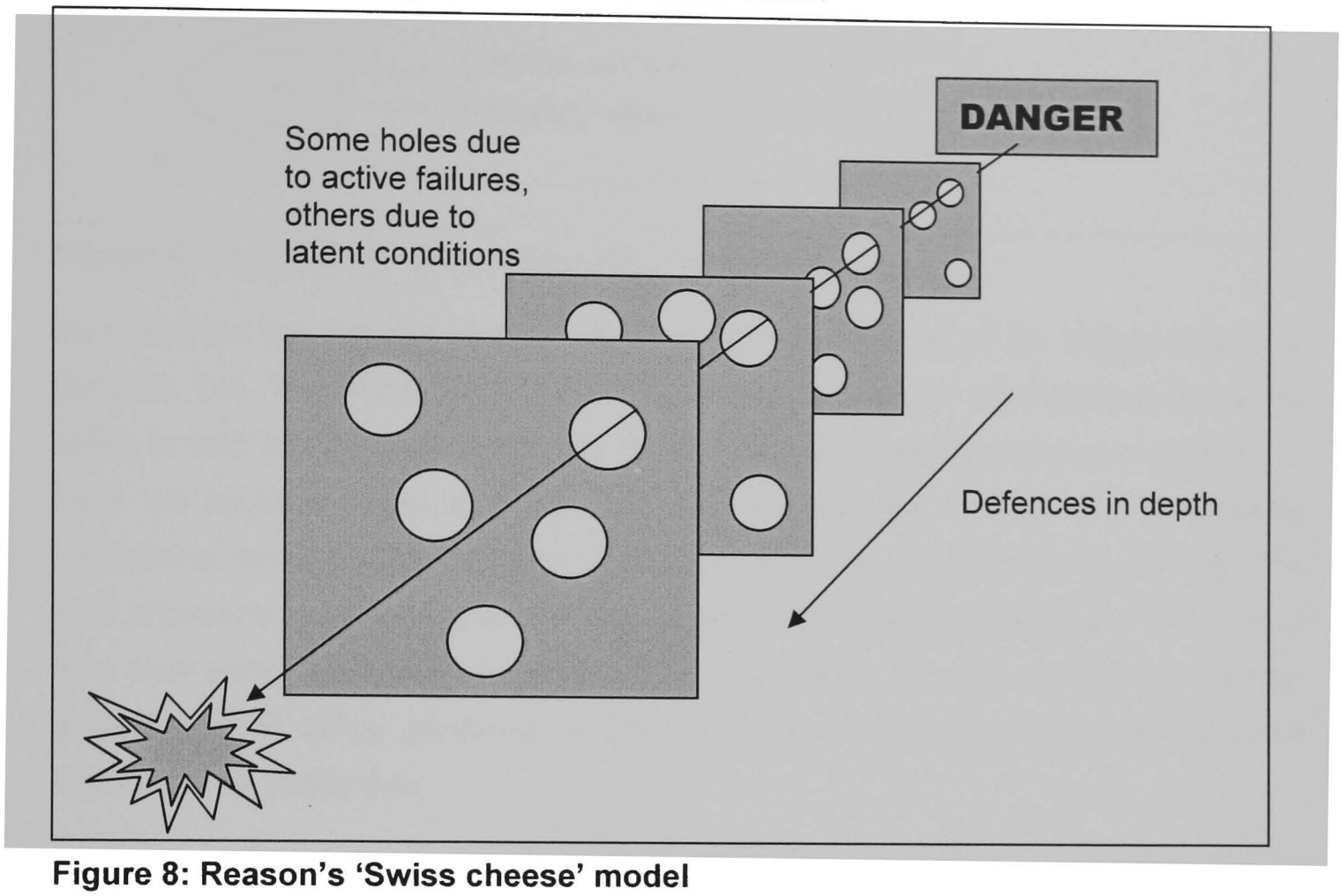


Figure 8: Reason's 'Swiss cheese' model

The defences in depth can be breached by 'active failures' or 'latent conditions'. Active failures are events such as component failures or procedural violations by front-line operational staff. Failure of a driver to stop a train at a red signal aspect is therefore a type of active failure that could lead to a train collision. A driver accelerating his train above the speed limit on a curve is an active failure that could lead to a train derailment. Latent conditions are generally organizational or procedural weaknesses further back in the causal sequence. Organizational accidents are a problem because, although in theory the breaching of all defences is highly unlikely, in reality there are processes at work that make such an occurrence possible, and in some cases highly likely.

Work activity to generate revenue ('production') and work activity to ensure safety ('protection') are dependent upon the same processes within an organisation. There is a continual conflict between these two types of activity. The occurrence of an accident tends to increase pressure on the company and its workers to maintain safety controls and safety performance improves. But this improvement is only temporary. Success will inevitably lead to a lack of awareness within the organisation about the occurrence of possible accidents. Over time, the organisation becomes complacent and production pressures are allowed to erode safety performance.

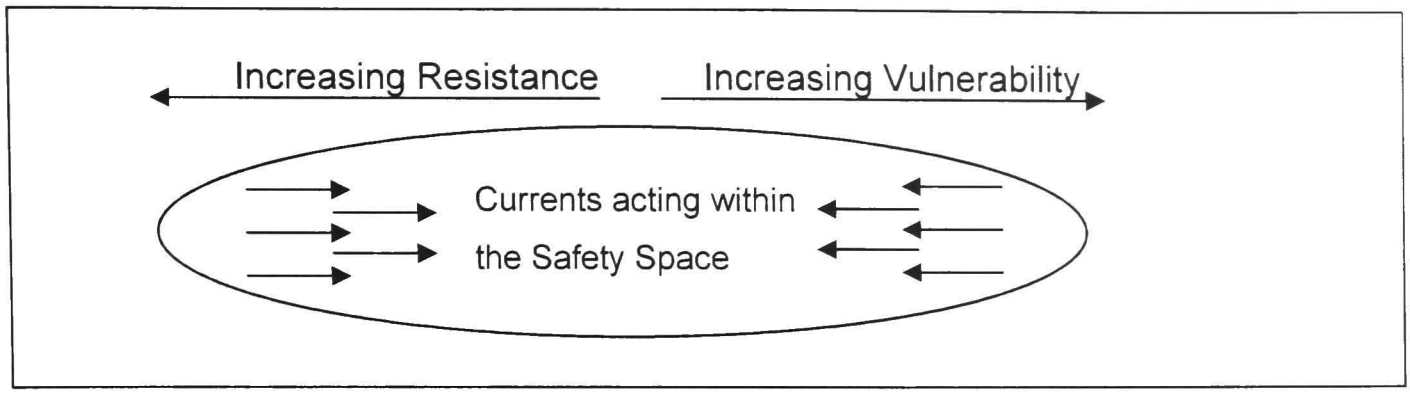


Figure 9: Countervailing currents within the safety space

Reason uses the diagram shown in Figure 9 and the concept of the 'Safety Space' to illustrate this. The basic theory here is that there are some organisations for which safety is 'bad' and some for which it is 'good'. The 'bad' organisations are more likely to have an accident. This accident, being an immediately obvious and undeniable measure of safety failure, leads to reactions to improve safety in the short term. The best organisations however, are lacking in measures of safety failure and hence over time their safety performance suffers. Production goals, because of their immediacy, gradually erode safety performance due to a lack of competing safety performance measures. He states that:

'Very few organizations occupy fixed positions within the Safety Space. Most of them are in continuous motion, either by being actively driven towards the resistant end of the space by energetic implementation of effective safety measures, or by being allowed to drift passively towards the unsafe end.'

Rasmussen expands on this idea arguing that over a period of time the relationship between protection and production in organisations inevitably leads to *'migration of activities to the boundary of acceptable performance'* ((Rasmussen 1997), page 190). This is because in large and complex systems the actions of people who need to work together to prevent the occurrence of accidents are functionally disconnected. Accidents are prevented by a variety of different people, in different locations, with a variety of tasks competing for their attention and priority. Over time they will adapt their behaviour according to their perception of the importance of their safety related tasks. If they have no visibility or understanding of accident causal sequences their perception is likely to be flawed. The pressures can cause safety defences to be eroded such that the conditions for an organizational accident substantially exist. All that is required to cause the accident in such circumstances is the final active failure that allows all defences to be breached.

Reason stresses that in order to 'navigate the safety space' and resist these pressures managers need 'navigational aids' to understand where they are in the safety space.

These aids are needed to help them understand how safe their organisation currently is, and where to resist production pressures so that performance is not eroded. Reason says:

'We need to learn the right lessons from past events, and then translate that knowledge into enhanced resistance. At the same time we must make visible to those who manage and operate the system the latent conditions and resident pathogens that are an inevitable part of any complex technology' (pages 116-117).

(Hale, Heming et al. 1997) and (Kirwan 2001) outline related interpretations of Organizational accident theory.

Accident occurrence on the UK railway network is now investigated. This will allow the relevance of organizational accident theory to the occurrence of such accidents to be gauged.

3.2 Accidents in the UK railway industry

The UK railway industry is relatively safe compared with other modes of transport. The graph of Figure 10 shows fatality rates across all major transport modes in recent years. It shows that in recent years rail is safer than all transport modes except air, when measuring safety as fatalities per billion passenger kilometres.

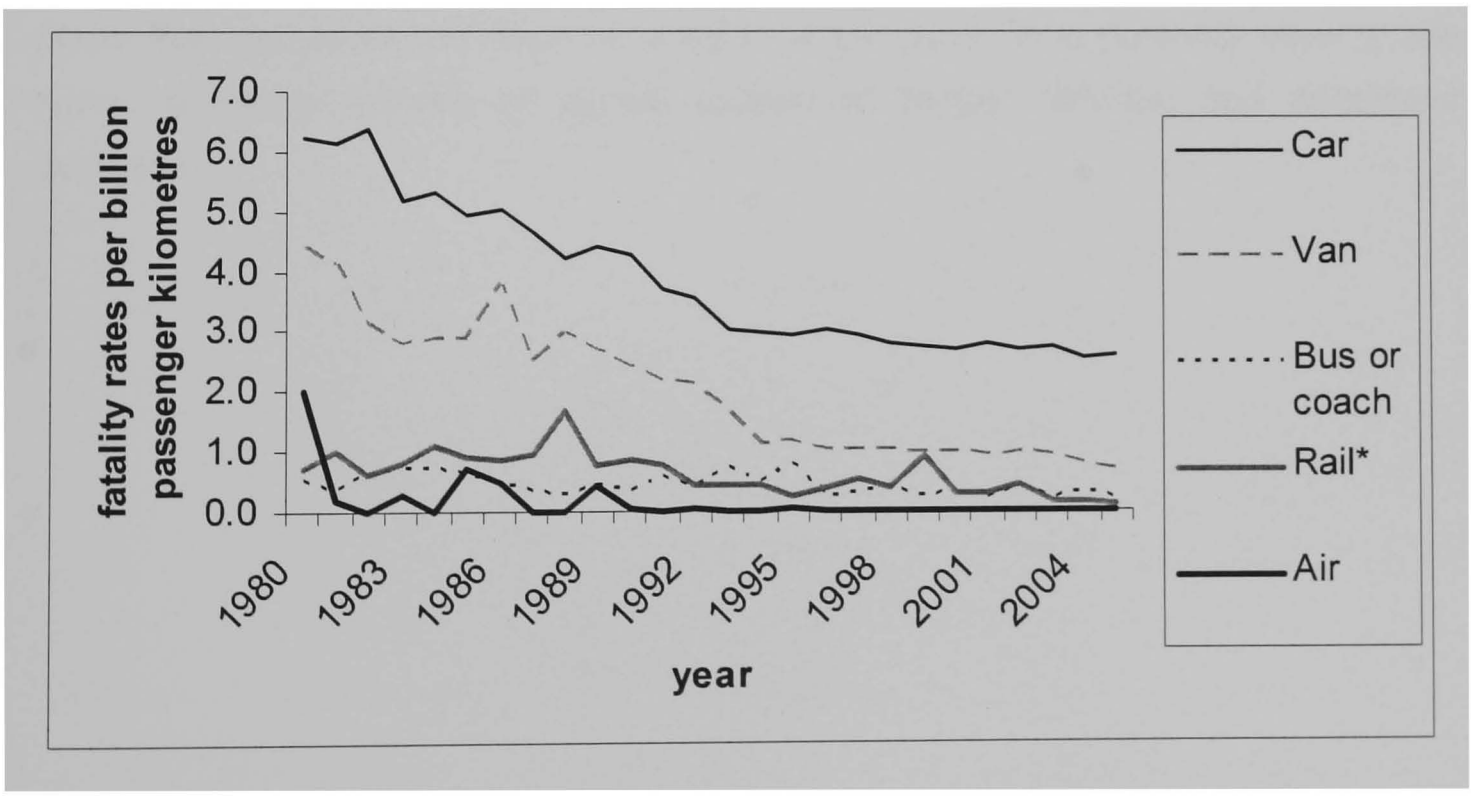


Figure 10: Passenger transport fatality rates in Great Britain (DfT 2007)

In particular rail travel is much safer that road travel by car. According to the Department for Transports 2007 estimates (DfT 2007) the fatality rate to railway passengers in 2006 was 0.1 fatalities per billion passenger kilometres whereas the

fatality rate for car drivers and passengers was 2.5 fatalities per billion passenger kilometres (a figure which is 25 times higher). However major accidents have always occurred on the UK railway network and continue to do so. These accidents are of a range of different types. An annual statistical analysis of fatal train accidents on Britain's railways is undertaken by the Centre for Transport Studies at Imperial College (Evans 2003). The latest report (Evans 2008) found that although performance on the railway was worse than in 2006, it was still in line with previous statistical predictions, and a general long term trend in the reduction of accident fatality rates.

3.2.1 Accidents and Incidents

The Safety Risk Model (SRM) developed by the Rail Safety and Standards Board (RSSB), lists 125 separate and distinct accident types that can occur on the UK railway infrastructure. These types of accident can occur to passengers, railway staff and members of the public, and range from trips and falls to train collisions.

Figure 11 shows the predicted 10 highest risk accidents in the UK railway industry, as estimated by the Rail Safety and Standards Board (RSSB 2006). The top five types of accidents all involve train movement. Accidents involving trains are usually those with the most severe consequences. Therefore they cause the most public and media concern and tend to be the accidents which drive the actions of the railway industry. Major train accidents that have occurred in recent years have generally been of two types: accidents caused by signals passed at danger (SPADs) and derailment accidents.

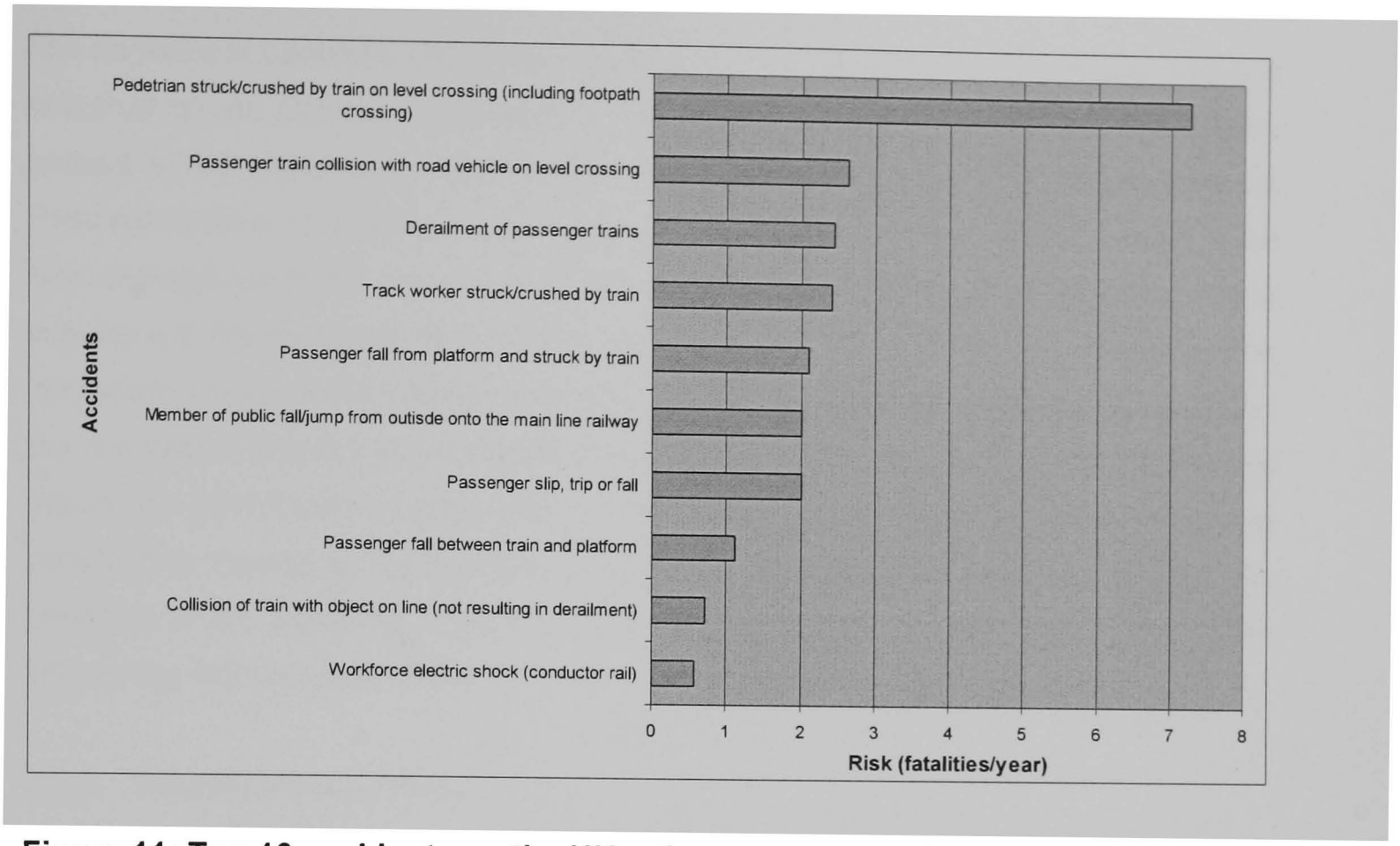


Figure 11: Top 10 accidents on the UK railway (RSSB 2006)

3.2.2 Signal Passed at Danger (SPAD)

Separation between trains is maintained through the use of lineside signalling. The location of the train on the track is detected electrically using track circuits which determine whether or not a train is present in each 'block section' of the line. A block section consists of the area of track preceding a signal. There also a small 'overlap' in front of the signal to prevent accidents occurring due to braking misjudgement. Where a track circuit shows that a block section is occupied the signal behind it is set to red, indicating that no other train should enter the block section.

The prevention of train accidents relies heavily on the driver being able to systematically interpret and react to the signalling indications shown to them. To support them in this task a number of items of equipment are used. The Automatic Warning System (AWS) sounds a horn, or a buzzer, in the driver's cab to indicate when the driver is approaching a restrictive aspect (either amber or red signals). The Train Protection and Warning System (TPWS) automatically applies the brakes of a train going past a red aspect.

If a driver goes past a red signal for any reason, the incident is known as a signal passed at danger (SPAD). Although most SPADs occur as a result of minor misjudgement of braking distances they have occasionally led to serious accidents. For example, in recent years major accidents have occurred at Ladbroke Grove (HSE 2000), Southall (HSC 2002) and Watford Junction (HSE 1998).

The accident at Ladbroke Grove was the most severe seen in the UK in recent years. It occurred on 5th October 1999 when a Thames turbo train travelling from Paddington passed a red signal and collided with a High Speed Train (HST) heading towards Paddington from Cheltenham. The closing speed of the accident was 130 mph. Fuel tank damage led to the release of six tonnes of diesel. As a result of the collision and subsequent fire thirty-one people died and a further 227 were taken to hospital. The immediate cause of the collision was that the driver of the Thames turbo did not obey the red aspect and in fact accelerated towards the signal. The accident led to a public inquiry by Lord Cullen (Cullen 2000; Cullen 2001) which identified many factors as contributory causes to the accident. These causes included factors ranging from the condition of the signalling infrastructure to the regulatory structure and culture of the UK railway industry as a whole.

3.2.3 Derailment accidents

A derailment occurs when a train becomes separated from the track guiding its direction of movement. Derailments are often minor incidents leading to damage to the track and train only. However they have the potential to lead to significant damage and injury if the train is going at substantial speed, hits a large object such as a building or another train, or if any train involved in the resulting accident is transporting hazardous of flammable goods. Derailments have a variety of potential causes such as broken rails, misalignment of rails and points, train wheel faults or driving of trains at excessive speeds. Three recent high profile derailment accidents in the UK railway industry were the derailments at Hatfield (HSE 2002a), Potters Bar (HSE 2002c), and Grayrigg (RAIB 2007). Derailments can also occur due to train collision with obstacles such as road vehicles, as happened at Ufton Nervet (HSE 2004) and Great Heck (HSE 2002b).

The Potters Bar accident occurred in May 2002 when the rear coach of a four-coach commuter train, travelling to Kings Lynn from Kings Cross, derailed on a set of points on the approach to Potters Bar station. The rear coach became detached from the rest of the train and crashed into the station platform. Seven people died as a result of this accident and many were injured. The UK safety regulator at the time, the Health and Safety Executive (HSE) determined that the immediate cause of the accident was that the points had been incorrectly maintained.

The Hatfield accident occurred in October 2000. An express train from London to Leeds derailed on a curve to the south of Hatfield Station. The left hand rail at this location fractured catastrophically. The locomotive and front two coaches remained on the track but the rear eight vehicles were derailed and the two rear coaches separated

from the remainder of the train. As a result of the derailment four passengers were killed and seventy people were injured. The HSE's view was that the 'direct cause' of the accident was poor rail condition. The rail had been identified as in poor condition, and should have either been replaced or had a temporary speed restriction applied to it.

3.3 Organizational accidents in the UK railway industry

In section 3.1 organizational accident theory was described, and in section 3.2 the occurrence of accidents in the UK railway industry was discussed. In this section the extent to which the theory can be used to explain accident occurrence in the industry, and the various related behaviours that the industry exhibits are investigated. This is done by reviewing the most catastrophic accident in the recent history of the UK railway industry, the Ladbroke Grove accident. The industry's response to this accident and the prevention of SPADs more generally are also reviewed. The following sections therefore provide support to hypothesis 1 that 'organizational accident theory provides an explanation for the mechanisms by which major accidents occur within the UK railway industry'.

3.3.1 An organizational accident on the UK railway: Ladbroke Grove

The accident at Ladbroke Grove was subject to extremely thorough investigation by the HSE (HSE 2000) and the Cullen inquiry (Cullen 2000; Cullen 2001). The key active failure was that the driver of the Thames turbo train failed to stop at a red signal. The AWS system in the turbo train was functioning but did not bring the train to a halt implying that the driver falsely acknowledged that he had noted the red aspect. A wide number of coincident causes, which in the context of organizational accident theory can be considered as latent conditions, were also identified.

Key amongst them were:

- The driver was inexperienced.
- The signal was difficult for drivers to sight.
- The signaller was operating under demanding time constraints: train movements in the Paddington area were being controlled automatically. A very quick response was required by the signaller to avert the accident. ultimately the signaller was unable to react in sufficient time.

The Cullen Inquiry report stressed that these contributory causes were symptomatic of underlying organizational and managerial weaknesses. Unusually the driver had been

recruited from outside of the railway industry, when the preferred option was to recruit guards or platform staff. Reports acknowledged that driver recruitment was difficult for Thames Trains. Commercial pressure put on train operating companies, would have made it very difficult for them to argue for cutting services due to a lack of experienced drivers. The Managing Director of another train operating company was sacked following a period of driver shortages (Harper 2001). The signal sighting problem indicated flaws in the actual signalling system and its ability to meet its design intent. The infrastructure had been subject to a number of upgrades since 1990 and it appears that these were undertaken without rigorous consideration of their effect on signal sighting. Hall ((Hall 2003b), pp86-93) commented that experienced drivers regarded the track layout and the signalling in the area, as it was by 1999, as very complex and requiring great care when driving. As well as causing signal sighting problems it was this complexity that complicated the signallers routing task. Hall believes that there was a lack of will on Railtrack's part to incur large expenditure by adopting the only real solution and moving the signal gantry, as this would have been expensive, time consuming and would have resulted in significant service loss for a substantial period of time on this route. The disincentives would have been considerable, as Paddington Station, and the routes out through Reading to the West Country, are a known bottleneck with a lack of diversionary routes. Another safety defence, for mitigating the risk from train accidents, is the crashworthiness of the train. The Thames turbo train did not have a high level of crashworthiness, resulting in high numbers of casualties amongst its passengers.

Ultimately, the Ladbroke Grove accident occurred because a range of different safety controls were not working effectively at a particular location, at a particular point in time. This happened because the production pressures on the organisations involved were gradually allowed to erode these controls until the point where there was a very high accident risk. The people responsible for each of these controls were largely ignorant of the link between them – the accident sequence that eventually occurred and its various causes. In addition there were certain attributes of the network that meant that any accident occurring there would be likely to have severe consequences. Trains travelled at high speed, passenger loading was high, and some of the rolling stock in the area was known to perform badly in collisions.

Useful knowledge about the potential 'active failures' and latent conditions' existed prior to the occurrence of the accident. Many of the various causes of the Ladbroke Grove accident were known at some level in the industry prior to the accident happening. A signal engineer believed the signalling layout was dangerous and reported this to

management at least four years before the accident (Webster 2000). Possible mitigation measures were also suggested but discounted for a number of reasons (Harper 2000). The signal that was passed at danger was one of the twenty two signals on the Railtrack network that had been passed at danger the most number of times (Hall and Wiltshire 2002). The driver's lack of experience was also known. However, despite the existence of all of this potential indicator data, sufficient action to manage the risk was not initiated or considered a priority at this particular location.

Organizational accident theory accurately describes the processes that led to the occurrence of the Ladbroke Grove accident. A number of defences against SPAD accidents existed, but in this location at this particular time they were all penetrated. In some instances it seems highly likely that production pressures were at the root of these failures.

3.3.2 SPAD incidents

As predicted by Reason's 'safety space' model, the Ladbroke Grove accident, and previous SPAD accidents such as the Southall accident, resulted in the rail industry investing huge efforts in the reduction of SPADs. Various-network wide initiatives were set up, such as the National SPAD Focus Group, the circulation of publications and videos to spread good practice and awareness of SPAD risk across the industry (Metcalfe 2006) and the adoption of 'defensive driving' practices by train operating companies (TOCs) (ATOC 2003). Industry cost benefit analysis found that, according to the decision making principles applied by the industry there was no requirement to install TPWS, or the more advanced system Automatic Train Protection (ATP). The 2002/2003 Railway Group Safety Plan (RSSB 2003b) estimated the cost of TPWS to be £10 million per statistical life saved. The industry benchmark for determining safety expenditure at that time was approximately £1.5 million, nevertheless the government decided that the additional expense was necessary and passed legislation mandating the fitment of TPWS at all junction signals and other signals deemed to be of high risk. This installation was substantially completed in December 2003. A further programme of fitment of TPWS+, an advanced form of TPWS for signals that are approached at higher speeds, was subsequently undertaken.

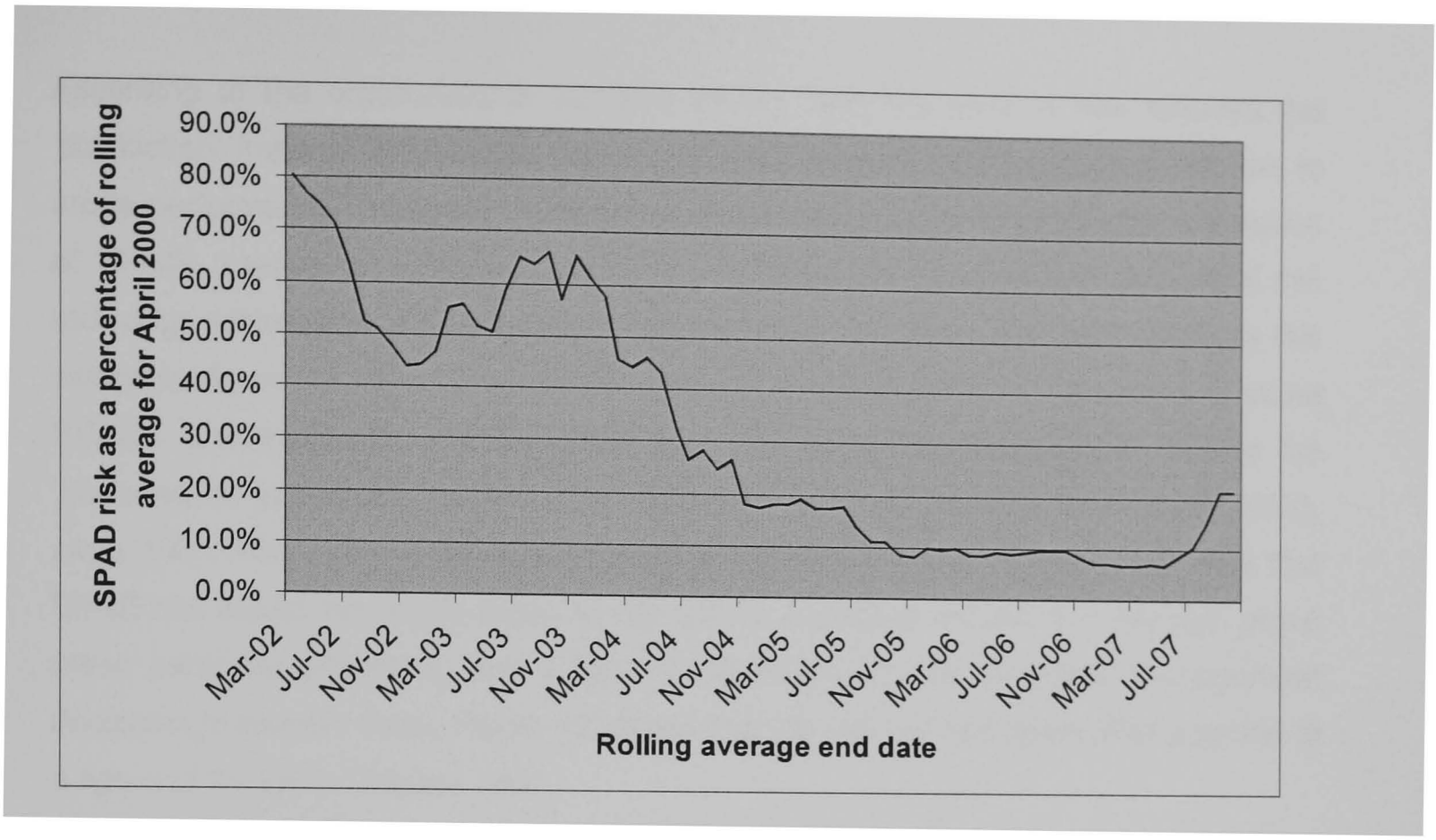


Figure 12: Rolling yearly total for estimated SPAD risk

Following the efforts of industry and government the incidence of SPADs decreased in the years following the Ladbroke Grove Rail accident. Figure 12 shows the reduction in estimated SPAD risk[5] over this period. The effectiveness of industry measures can be clearly seen. Estimated SPAD risk was reduced sharply until early 2002, whereupon it began to rise again briefly, before falling to historically low levels in late 2005.

From October 2005 to June 2007, the estimated SPAD risk was maintained below 10% of the initial baseline figure. According to organizational accident theory this time would have been one of vulnerability for the industry. As the rate of SPADs had been reduced there was much less incident data to use to help estimate and manage risk. Also the impressive reduction seen in SPAD risk had been achieved through a huge investment of resources. A number of industry wide initiatives were needed to achieve the reductions seen in SPAD risk. It is known that some of this investment was not considered cost effective by the usual standards of the industry. This investment occurred in a post-accident climate, where media interest in railway safety and in SPAD prevention in particular was high, and railway safety had been high on the political agenda as evidenced by the government intervention to install TPWS.

---

[5] The SPAD risk figure has been estimated by Network Rail using the SPAD risk ranking tool. This tool provides a metric based on certain conditions which are known to have the potential to increase SPAD risk, such as the speed of trains. The model itself is not in the public domain.

According to the organizational accident theory, with the level of risk reduced the 'production' impetus is lessened, leading to the potential for production pressures to erode performance. As some of the safety gains had been achieved by the imposition of TPWS, a technical system, it might be concluded that a significant amount of risk reduction achieved was permanent. However, many initiatives that contributed to this safety performance, such as defensive driving techniques, raised awareness about SPADs, and improved reporting were more susceptible to erosion over time to the 'boundary of acceptable performance' described by Rasmussen ((Rasmussen 1997), page 190). After achieving these substantial improvements it would be expected that SPAD risk would eventually begin to rise due to a gradual reduction in concern about these particular accidents, and a lack of information to use to inform management decisions to prevent them. Figure 12 shows that the risk did rise again after a period to a figure of 21.3% in October 2007.

The discussion in sections 3.3.1 and 3.3.2 provide evidence that the mechanisms by which the Ladbroke Grove accident occurred, and the subsequent industry response to SPAD risk, are consistent with organizational accident theory. This supports hypothesis 1 that: 'Organizational accident theory provides an explanation for the mechanisms by which major accidents occur within the UK railway industry'.

3.4 Managing organizational accident risk

In this section, I consider what organizational accident theory tells us about how to manage the risk from organizational accidents. The potential problems or difficulties that might arise when applying the suggested concepts and principles in the UK railway industry are also considered.

3.4.1 Applying the theory

If it is accepted that organizational accident theory is applicable to the UK railway industry, how then could the risk from these types of accident be managed? As was discussed in section 3.1, the theory says that to protect against the occurrence of such accidents navigational aids are needed.

Risk models, and the causal data that supports them, are possible examples of the 'navigational aids' to which Reason refers.

In section 2.3, the various categories of accident cause that are used in this thesis when discussing risk analysis, assessment and modelling were outlined. These causes were categorised as events and conditions. These causal types can be related to the

various elements of the 'Swiss cheese model'. The accident trajectory is the sequence of events (or active failures) that lead to the occurrence of an accident, whether a human error, a technical failure or an external event. The conditions can be thought of as the 'latent conditions' whose existence increases the likelihood of occurrence of one or more 'active events' in the accident sequence.

Organizational accident theory therefore implies that up to date knowledge of the existence of conditions, and whether or not some events in the accident sequence have occurred is needed in order to understand whether an accident is likely in a particular situation. Such information (hereafter referred to as 'safety indicators' or safety indicator data') can be used to monitor safety performance to help understand where and when the potential for organizational accidents has arisen.

3.5 Accident risk management in the UK railway industry

In this section, I review how the risk from major accidents has been managed in the industry over recent years. This review highlights the difficulties and potential benefits of applying the management principles of organizational accident theory in the UK railway industry. This discussion further illustrates how organizational accident theory can be used to describe and interpret real phenomena in the industry (this further supports Hypothesis 1). The review also informs the development of the ideal risk modelling requirements that are proposed later in the chapter (see section 3.7).

3.5.1 Managing train derailment risk

The biggest single identified cause of derailments is track faults and since the Hatfield accident there has been considerable expenditure on improving track quality. The National Audit Office reported that total expenditure on Britain's railways was predicted to be 30% higher due to track renewal work in the years following the Hatfield accident ((NAO 2004), p2).

Following the major derailment accidents at Hatfield and Potters Bar, and the additional expenditure that followed it, the incidence of derailments of all types fell (see Figure 13).

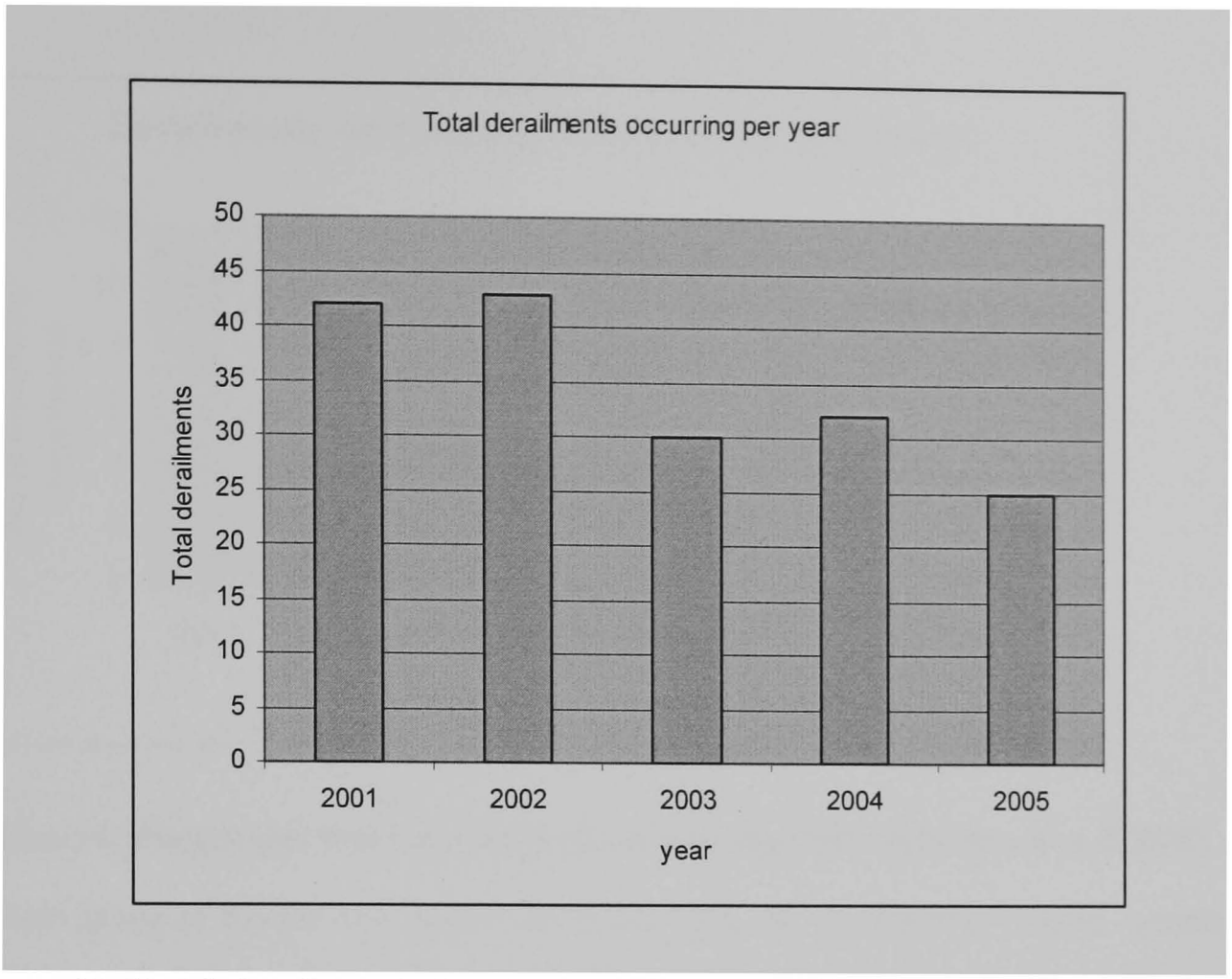


Figure 13: Total derailments (or all types) between 2001 and 2005 (source RSSB)

However, it is unclear whether this reduction actually resulted in the reduction of derailment risk across the network. A downward trend in the occurrence of derailments does not necessarily translate to an equivalent reduction in risk. It can be seen from Figure 14 that, during the period in which derailments of all types were reduced, reportable passenger train derailments remained fairly constant. A significant proportion of the reduction in the occurrence of derailments was achieved by a reduction in freight train derailments.

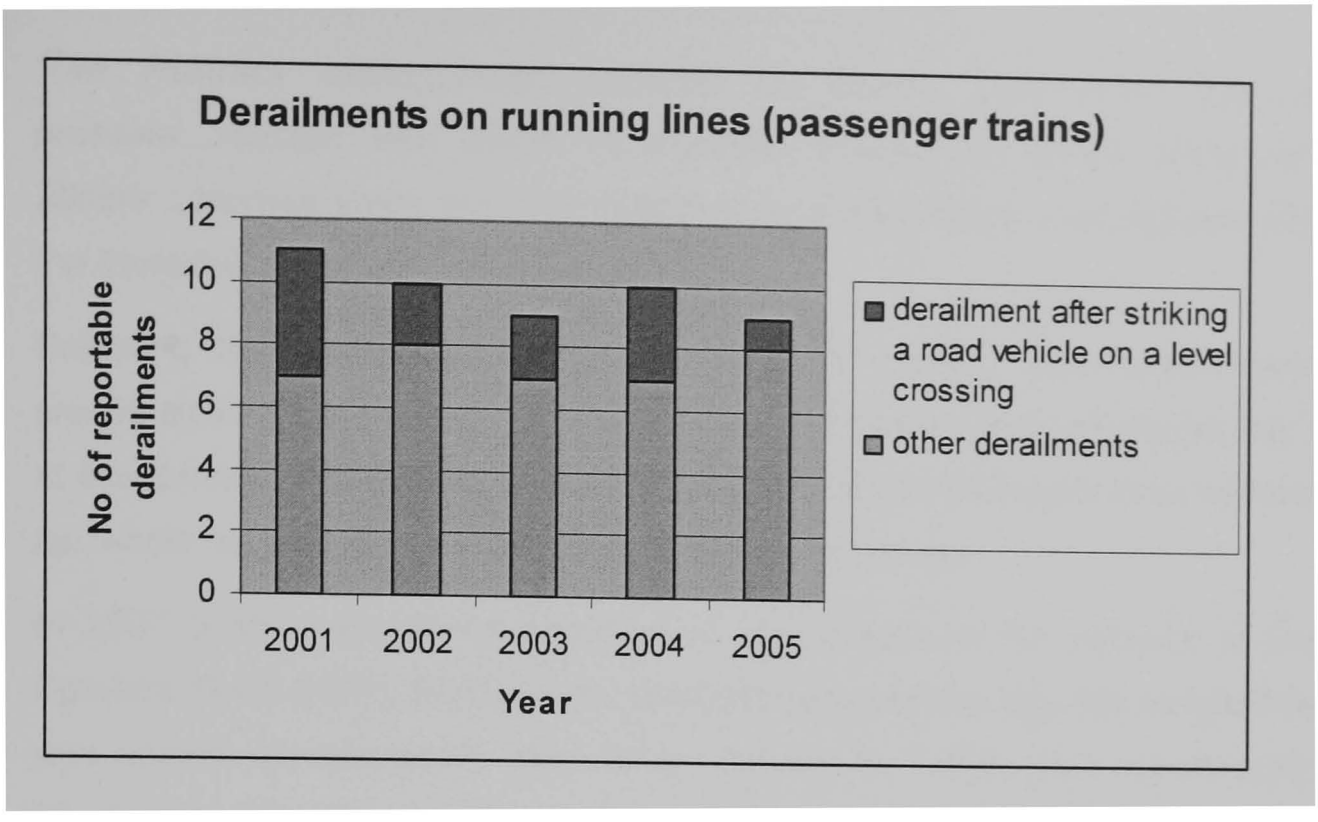


Figure 14: Passenger train derailments occurring 2001-2005 (source RSSB)

Certain types of freight train which have two-axle, as opposed to bogied, wagons are highly susceptible to derailment on poorly maintained track. Freight trains do not carry passengers, and tend to travel at lower speeds than passenger trains. This means that freight train derailments generally have less severe consequences than passenger train derailments. Therefore, it is unlikely that the reduction in freight train derailment will have resulted in an equivalent reduction in risk.

The industry response has tended to focus on poor track quality, the most obvious and easily identifiable cause of derailment incidents. However, derailment accidents have a wide variety of causes such as wheel faults, driver behaviour and obstructions on the line. Information relating to such causes is not readily available in asset records and has to be obtained, often by manual inspection or monitoring. It is also difficult to baseline. Faults are constantly evolving, and obstructions may only exist for a short period of time. However, as has been discussed, information about all causes is essential to the determination of levels of derailment risk and the prevention of organizational accidents. The other thing which is key to risk are the operational conditions of the network such as the speed of trains, the number of passengers on each train, and the number of trains using a section of the network.

Without all of this relevant information, and a means of interpreting its meaning to risk at each location on the network, it is difficult to target resource to effectively reduce derailment risk. The difficulties with managing derailment risk, and the problems that they caused in the aftermath of the Hatfield accident, were clearly expressed by Rod Muttram, the former Chief Executive of Railway Safety, the forerunner to RSSB.

'The Railtrack management, battered by media, government and regulatory pressure...reacted with panic. It imposed emergency speed limits as low as 20mph...Journey times became extended to a completely unacceptable degree and the timetable collapsed.' (Muttram 2003)

Following the Hatfield derailment accident the industry was under huge political pressures to act, but lacked sufficient insight into how to effectively target risk reduction at derailments. The industry therefore applied control measures indiscriminately across the whole network with severe operational consequences.

In 2007 another derailment occurred at high speed on the network at Grayrigg in Cumbria (RAIB 2007). Although the accident potential was high the accident resulted in less severe consequences than either Hatfield or Potters Bar resulting in a single fatality. However, the accident illustrates that the UK railway network is still prone to the occurrence of major derailment accidents.

The discussion here supports an argument that the inability to systematically collect and interpret indicator data relating to the causes of derailments has undermined the ability of the industry to manage derailment risk. This is a serious problem which has been shown to create huge problems for the industry.

3.5.2 Managing SPAD risk

I now consider how the industry has managed SPAD risk. As with the review of derailments, this review indicates the problems of managing the risk from organizational accidents in the UK railway industry. Following the Ladbroke Grove accident huge effort was invested in SPAD prevention by the industry, with some success. Therefore, the industry's response to SPAD risk provides some insights into how risk might be managed more effectively.

Figure 15 shows the rolling yearly total for SPADs occurring on UK railway infrastructure. The graph shows a gradual, but not dramatic, decrease in the number of SPADs occurring over this period.

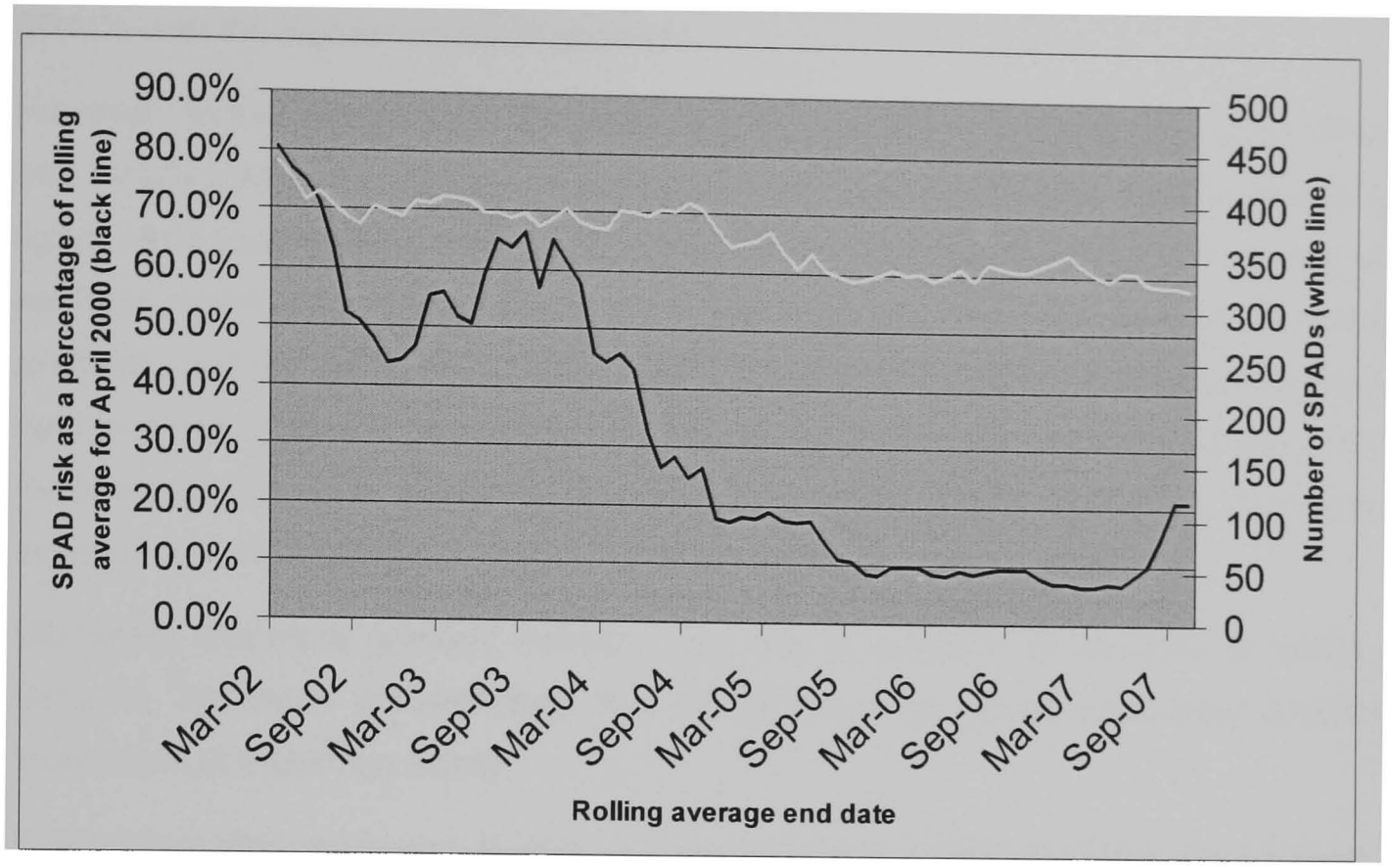


Figure 15: Rolling yearly SPAD total and Rolling yearly average SPAD risk

The graph of Figure 15 shows that the trend in estimated risk from SPADs is entirely different from the trend in SPAD occurrence over the same time period. In general, the reduction in risk has been much greater than the reduction in SPADs. The graph implies that the industry has been able to target its activity to reduce the occurrence of SPADs with the most risk potential.

It is possible to differentiate between SPAD occurrence and SPAD risk reduction, as shown in Figure 12, because the railway industry has some knowledge of the conditions on the network that are strongly correlated to underlying levels of SPAD risk. SPAD risk can be quite closely correlated to particular track layouts, and the speed of trains. This information can be collated from planning information and asset records. However such information is only of use if a model exists, to use the information to estimate and monitor risk. The SPAD risk ranking tool was developed to do just this and is available to those taking decisions about how to invest in SPAD risk reduction. Therefore measures can be targeted at locations and situations with the highest estimated risk. As has already been mentioned, TPWS was first installed at signals protecting junctions, as SPADs at these locations might lead to train collisions, and therefore create the potential for catastrophic accidents. Next TPWS+ was installed at signals where trains often passed at high speed. Train speed obviously provides a good indication of risk as it influences both the likelihood and the severity of an

accident. Using this information it was possible to target measures at the prevention of SPADs with the highest accident potential.

However, further information, and improved risk models would still be useful. TPWS was initially installed at all junction signals. Where these installations were to signals on lightly used lines, with no timetabled conflicts between trains at junctions then they will not have contributed significantly to risk reduction. If this information were more readily available, and the model were better able to utilise it, perhaps these installations would not have been made. In fact the railway industry is seeking the removal of many TPWS installations that now seem inappropriate, given new data based on operational experience (ORR 2007).

Ultimately, the more relevant indicator data that is available in advance of taking a decision, the more discriminating the industry can be about proactively targeting investment at improving safety.

In summary then, success has been achieved in the reduction of SPAD risk because it has been possible to target key measures like TPWS at high risk locations on the network. Some key indicators of SPAD risk are known, and happen to be able to be monitored. Models are available to interpret these indicators and this knowledge is used to support decision making. This lends support to the idea that better indicator data, and risk modelling tools can provide the 'navigational aids' to which Reason refers. However, even though targeting has been effective for the management of SPADs, better indicators would have allowed more effective targeting of control measures and hence more effective investment. More generally, organizational accident theory says that to improve safety further better indicator data is needed. This implies detailed causal analysis and knowledge of the state of infrastructure and the performance of people at all locations across the network.

3.6 Problems applying organizational accident theory in the UK railway industry

The review of derailments and SPAD incidents highlights that safety indicator data relating to the potential causes of organizational accidents is often not readily available in the industry. When information is available, there are not always models available which can use this information to estimate risk and therefore support management action. This section investigates why this might be the case and explores some of the reasons why it is difficult to apply organizational accident theory in the UK railway industry in practice.

In the UK railway industry the identification, collection and analysis of safety indicators is complicated for a number of reasons.

- Because the industry operates with high levels of safety there is little readily available accident data with which to ascertain the effectiveness of defences against accidents, at any given point in time.
- Major accidents are often the result of a complex set of causes that are particular to a location or situation. Data relating to the variety of causes that might be implicated in a major accident is not routinely monitored.
- The sheer size and variability of the railway network means that the amount of potentially relevant data is vast. This makes collection and interpretation of data very difficult.

These three issues are investigated further in sections 3.6.1 to 3.6.3.

3.6.1 Lack of safety indicators

RSSB maintains the Safety Management Information System (SMIS) database to record details of events reported to them by the various railway companies. This information is used to support RSSB's risk modelling, and also the development of industry reports such as the annual safety performance report (RSSB 2007a). The requirements for data reporting are described in a RGS 'Reporting of Safety Related Information' (RSSB 2007c). SMIS requires railway companies to report:

- All accidents resulting in death or injury
- Dangerous goods incidents
- The occurrence of a wide range of 'safety events'. These include hazards such as derailments but also other events further back in the causal sequence such as train overspeeds, track faults and train faults.

The standard requires that for all 'safety events' the company:

'shall be responsible for ensuring that details of the immediate cause (s) and where appropriate, the underlying cause(s) are included in the SMIS record of the event.' ((RSSB 2007c) page 12)

The standard defines an immediate cause as 'an unsafe act or condition which causes an accident or incident' ((RSSB 2007c) page 6). An incident is separately defined as a 'near miss'. This definition therefore implies that 'safety events' are incidents or accidents (and not the events or conditions preceding them).

The definition of an underlying cause also implies that 'safety events' are incidents or accidents. An underlying cause is:

'any factor(s) which led to the immediate causes of accidents or incidents, or resulted in such causes not being identified or mitigated ('(RSSB 2007c), page 33).

According to the definitions of cause outlined in section 2.3 the 'underlying cause' might relate to an event preceding the event of interest or a condition whose state correlates closely to the event. The standard does not mandate the recording of 'underlying cause(s)' unless the event being reported has been the subject of a formal investigation. Taking all of these definitions into account there is some room for interpretation in the application of the standard. However there is only a firm requirement to record incidents and accidents.

Major accidents on the UK railway network are mercifully rare. However, detailed analysis of the causes of major accidents is generally only undertaken in such circumstances. As a result of this, detailed causal data for potential accidents is scarce. This issue has been recognised as a general problem in the safety field for many years. Heinrich (Heinrich 1931; Heinrich 1951) describes a model of the typical ratios between severe accidents, minor accidents and incidents (called no injury accidents). The model is shown in Figure 16 and visually highlights how, for every major accident that occurs there are a large number of more minor accidents or incidents. As you go down the triangle, from accidents to incidents more data is available. This theory maps well to the railway industry.

There are a wide range of accidents and incidents that occur due to the operation of the rail network. At the lower extreme are events like passenger slips, trips and falls at stations. These occur very regularly, and therefore there is a lot of occurrence data available relating to them. This makes it easier to estimate their future likelihood of occurrence. Slips, trips and falls also tend to lead to similar outcomes that are typically of low severity. Past data, collected at the network level, concerning the frequency and severity of these types of accident is therefore likely to be highly indicative of future risk. However at the other extreme, there is the potential for major train accidents to occur. Major train accidents are rare and therefore there is little hazard and accident data available to support their analysis. The severity of major train accidents can also vary widely, introducing further uncertainty. The Southall and Ladbroke Grove rail accidents could be considered to be similar in many respects. However, the former resulted in seven fatalities whereas the latter resulted in 31. Past data relating to the

occurrence of major train accidents does not provide a clear indication of the actual risk they present.

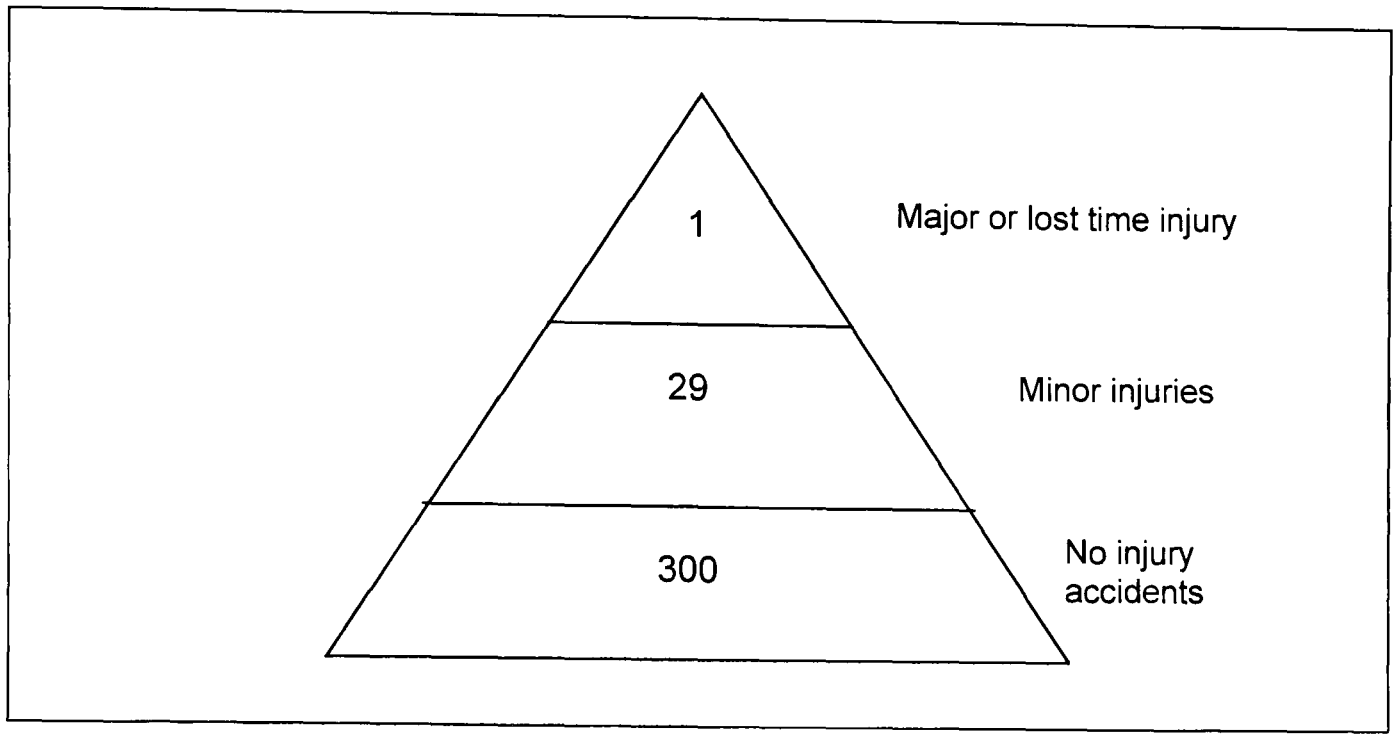


Figure 16: Heinrich's accident triangle

3.6.2 Problems with data collection

As discussed in the previous section, the RGS for reporting of safety related information requires only that the 'immediate cause' of any accident or incident should be recorded. The various causes of an accident were outlined in section 3.3 and consist of both events and conditions. This immediate cause could be an event of any type, a technical condition or an operational condition. It is unlikely to be an organizational condition as these types of failing are generally followed by an 'active failure' which would more clearly be considered the 'immediate cause'. For example there were organizational failings in the process by which the driver of the Thames turbo was recruited prior to Ladbroke Grove accident. However this would not be considered an 'immediate cause' according to the definitions in the RGS as it triggered, and was followed by, a number of other failings the last of which was the driver passing the red signal. Performance conditions are also unlikely to be reported as the 'immediate cause' of an incident. Performance conditions which are strongly correlated to risk like train speed are not necessarily deviations from the planned operational parameters of the railway. Performance conditions (like train speed) would not be recorded as causes unless performance limits are being exceeded (e.g. a train overspeed).

Data is collected for a variety of different reasons in the rail industry. In addition to the standard mentioned data is collected for performance monitoring, to support

compensation payments and to meet specific reporting legislation. It is also collected by various organisations to support prosecutions. Data collection is therefore not generally scoped for the development of detailed risk models. Stoop (Hale, Wilpert et al. 1997), page 77, points out that in general data used for analysis in safety critical industries is vulnerable to underreporting, incomplete recording, and does not necessarily provide the researcher with the complete picture of the conditions under which the accident took place.

The latter point is particularly true for the railway industry. Many of the factors that it is known risk is sensitive to are not routinely monitored. This results in a loss of context for the data. Data is available and may be collected. However the models that exist are not able to be used to interpret the type of data that is available. This is a general problem. Hale and Koorneef point out that it is difficult for those recording data to ensure they record all information that is necessary to improve safety.

'Any report, by its choice of words simplifies real-life processes and conditions. It is impossible to know just on the basis of the data provided in the notification report whether or not crucial context data are missing and if so, which data. It is like looking into a room through a keyhole: one cannot see what is out of sight, but possibly relevant for understanding the visible scenes.' (Koornneef and Hale 2001).

Reports do not tend to provide all of the information that is needed.

3.6.3 The spread and variability of the railway network

The UK railway network exists over a wide geographic area and consists of over 20 thousand miles of track. A hazard, such as a train passing a signal at danger, may occur at many different locations on the railway. Although broadly the same sequence of events would need to occur for this to happen at each location, the probability of these events occurring will differ widely depending on the effectiveness of the safety controls in each location and local conditions.

In order to understand the risk across the network, safety indicator data for each possible location on it is needed. If, as stated in the previous section, the full accident causal sequence across all locations on the network is to be considered then substantial data collection and monitoring is required. This data would also need to be interpreted to identify where risk is highest at any given time. This makes data management and analysis much more complex than it would be in a single location, like for example a single nuclear power plant, or oil platform, or indeed a single railway station.

At Ladbroke Grove it was known that the signals were difficult for the driver to sight for a variety of different reasons. It was also known that the driver who passed the signal at danger was inexperienced. In most other locations neither of these conditions hold true and both are true in even fewer. However there was no process or model being systematically applied to interpret the relationship between the state of these various indicators and the degree of accident risk. The integrity of all of the various defences that were needed to prevent it had not been jointly and holistically considered in advance of the accident. The focus of the railway should clearly be on identifying such situations in advance of the occurrence of a major accident. This principle has been advocated by Health and Safety Executive in guidance for its inspectors (HSE 2001a).

'Location by location consideration of risks should however be carried out to determine whether, even if application of a control measure system-wide would be ruled out on the grounds of excessive costs, application is reasonably practicable in certain locations, such as those that present a particularly high risk and/or low cost.'

However, the HSE does not comment on how onerous a task this would be for the consideration of all types of accident risk across the network as a whole. There are a huge number of separate locations on the network where accidents are possible. There are also a huge number of possible accident sequences to consider. To analyse them all, from first principles, would be a major task. And as the integrity of these defences may be constantly changing, due to performance pressures for example, it would be an ongoing task.

The concept of the 'safety space' (see section 3.1) and the issue of large geographic scope combine to create an additional problem for railway safety management – the presence of 'risk hotspots' – locations on the network where risk is disproportionately high.

The UK railway consists of many different locations, organisations, technologies and procedures. It would therefore appear to be inevitable that this variability would result in a wide variability in accident risk across the network. The graph of Figure 15 provides support for the existence of 'risk hotspots' on the UK railway network. It shows that the estimated risk has reduced significantly from only a small change in the number of SPAD incidents. The rise in SPAD risk seen in late 2007 has occurred fundamentally because of the occurrence of two high risk SPAD incidents (from a total number of 322). It can be seen that recently the risk has risen whilst the number of incidents in total has reduced.

This variability is predicted by organizational accident theory which argues that safety performance varies greatly between organisations because of continual movement in the 'safety space' The organizational pressures that drive movement in the safety space are significant in the industry and one might expect these forces to result in a wide variety of safety performance. As was discussed in section 3.1 Rasmussen expands on this theory to say that the production pressures in an organisation inevitably drive organisations to the point where accidents are likely. One might consider that the accidents at Ladbroke Grove and Hatfield are examples of this. Another factor to consider is that when accidents occur resources are heavily diverted to particular areas of risk. This mechanism was clearly seen in the aftermath of the Hatfield accident. In practice the railway has limited resources to invest in safety. If one type of accident receives a disproportionate share of these resources, then it is likely that safety will suffer in some other area. If this were the case we might expect to see accidents occur due to different causes as a result of money being diverted to manage risk related to accident which happen to have occurred in the recent past.

Risk varies significantly across the network, from location to location. Those locations with the highest risk are referred to in this thesis as 'risk hotspots'. It may well be that, in a number of locations, at any given time the conditions under which a major accident could occur exist. All that is required is the failure of a single line of defence. If this is the case then the management problem is how to identify these locations and intervene before an accident actually occurs.

In summary, management of safety on the UK railway is greatly complicated by the large geographic spread of the railway and the variability and complexity that occur as a result of this. Huge amounts of information are potentially relevant to the management of safety and monitoring and analysing all of this information would be a major task. The performance of the railway is variable from location to location and in some locations – risk hotspots – risk is disproportionately high.

3.6.4 Summary of problems

Accident and incident reports are the only indicator data that are definitely collected by the industry. However, because major accidents are rare in the UK railway industry (as outlined in section 3.6.1) there will not tend to be significant amounts of such data. Reporting tends to be done for a variety of reasons and might not provide all of the required causal information even where reports are available. The problem of monitoring and interpreting the meaning of safety indicators in the UK railway industry is compounded by the size, variability and complexity of the network which means that

huge amounts of safety indicator data, relating to possible accident causes would need to be collected. However there is a need to undertake such monitoring and analysis as at any given time there will be a number of locations on the network where risk is disproportionately high. It may well be that an organizational accident is imminent at such locations.

3.7 Ideal risk modelling requirements

In this section a number of ideal requirements for risk models are stated given:

- Hypothesis 1 – that Organizational accident theory provides an explanation for the mechanisms by which major accidents occur within the UK railway industry – is valid
- the particular problems of applying organizational accident theory in the UK railway industry, as identified in section 3.6.

The derived requirements define the ideal characteristics of risk models referred to in Hypothesis 2.

3.7.1 Requirements for a model to support the management of organizational accidents

I have argued that major accidents in the railway industry exhibit the properties of organizational accidents. Organizational accident theory provides a conceptual model to use as the basis of a risk model, and also with which to identify safety indicator data that could usefully be collected.

Safety indicator data relates to the range of different causes of an accident. An accident ultimately occurs because of a particular sequence of events. There are also various conditions, which influence the occurrence of the events and the severity of any accident. These conditions might indicate latent weaknesses in an organisation's defences or they might relate to the operational characteristics of the network that indicate high risk, such as train speed. The way to achieve continuing safety improvement is to understand all of these underlying causes of accidents by analysing the accident event sequence. These causes will, by definition, occur more regularly than the accident itself, providing improved opportunity for collecting data and developing indicators.

A conceptual model is needed to interpret the meaning of this information for each possible major railway accident scenario, in each possible location on the network and to provide greater visibility of the accident sequence.

Organizational accident theory therefore implies the following ideal requirements for a risk modelling approach, which form the first two requirements elaborating upon hypothesis 2:

RMR1: Risk models should allow as many of the events in an accident sequence to be modelled as is practicable.

RMR2: Risk models should allow as many of the significant and quantifiable technical, operational, organizational and performance conditions that cause accidents or exacerbate risk to be explicitly modelled as is practicable.

The UK railway network is very large, consisting of many locations, organisations technologies and procedures. Although broadly the same sequence of events would need to occur for an accident to happen at each location, the probability of these events occurring will differ widely depending on the local conditions, which might relate to the integrity of safety defences or key operational parameters.

A model is needed which is able to represent the variety of conditions that exist from location to location across the network, and relate these to the accident causal sequence. Such a model could be used to identify the indicator data from across the network that should be monitored. It could also be used to estimate risk from this indicator data to identify the particular locations where risk was disproportionately high. This leads to the third recommendation elaborating upon Hypothesis 2.

RMR3: Risk models should be parameterised by conditions so that the risk at different locations and in different situations on the railway network can be rapidly recalculated.

3.7.2 Risk models and safety management

As was stated in section 2.1.4 safety is managed by railway staff according to a management system. A fundamental principle of SMSs is that they should be risk-based. In aviation SMS guidance, CAP712 (CAA 2002) Safety Management is defined as 'the systematic management of the risks [of aviation activities]'.

The elements that comprise the SMS must be focussed on identifying and managing risks. An organisation's risk model can therefore be thought of as the safety management system's brain. Organisation and planning are about ensuring that that the SMSs limbs are coordinated with what its brain is thinking. The monitoring, auditing and review elements of the SMS are its senses which must correctly inform the brain about the factors which will affect the level of risk. Therefore, the risk model and the various elements of the Safety Management System should be fully integrated together.

Risk assessment and modelling are critical to the management of safety. It is also critical that the risk information is understood and acted upon by those that take safety related decisions in the industry. To manage safety, an effective and up to date understanding of risk must be built into the management system and the practical actions of the company. In particular when the industry decides what procedures, plans and actions to put in place to meet its legal duty it must do so with an awareness of risk.

This leads to the next requirement for risk models:

SMS1: In order to ensure that they effectively support the management of safety, the uses of risk models should support the various stages of a safety management system.

This requirement can be broken down into more specific points by considering each of the various stages of a Safety Management System as outlined in section 2.1.4:[6].

- Organisation
    - Able to be used to gauge the impact of organizational changes on risk.
- Planning
    - Estimates the total network wide risk.
    - Allows ranking of risk by individual location or situation, to allow prioritisation and targeting of interventions.
    - Estimates changes in risk level following interventions.
- Monitoring (active)
    - Monitoring of changing network risk profile.
    - Monitoring of changing risk in each location on the network
- Monitoring (reactive)
    - Can be used to help learn lessons from accidents.
    - Can be used to diagnose the causes of accidents.
- Audit
    - Ability to be used to interpret audit results, and their implications for risk.

---

[6] No credible or specific support for the policy or review elements of a Safety Management System have been identified

3.7.3 Risk models and safety decision making

As was discussed in section 2.1.3, the railway industry guidance document 'Taking Safe Decisions ' (RSSB 2008b) describes how the industry uses risk information within the wider decision making process. The guidance stresses that risk modelling and analysis is not purely an analytical exercise but also has a more qualitative, judgment based element. The process of safety analysis has benefits above and beyond any numerical output that it produces, as it ensures that the domain experts think about the relevant issues in a systematic and structured way before reaching any judgment about what measures to put in place. Ultimately the intention of risk analysis and modelling is to assist the decision maker in best understanding the risks, costs and benefits of a particular decision so that an informed judgement can be made.

Risk models do not themselves improve safety. Safety is improved by the actions of managers and other railway employees. This leads to the final requirement for an ideal risk model.

SDM1: In order to ensure that they effectively support the taking of safety related decisions, risk models should be developed to be accessible to and understandable by those who actually manage safety on the network

3.8 Chapter summary: Restatement of ideal requirements

In this chapter, the recent accident history of Britain's railways was reviewed. The review found that organizational accident theory explains many of the phenomena seen in the industry. The theory provides an explanation of the causal mechanisms by which the Ladbroke Grove accident occurred, and how the various causes arose. It also describes the industry's response to major accidents more generally and provides an explanation for trends seen in reported accident levels in the industry.

The theory also proposes an approach for the management of the risk from organizational accidents. Consideration of these approaches again provides useful insights into why the industry's responses to previous actions may have (section 3.5.2) and may not have (section 3.5.1) been successful. The review led to the conclusion that there are three fundamental problems with the application of organizational accident theory to the management of risk in the UK railway industry:

- Lack of safety indicator data
- Problems with data collection
- The size and variability of the railway network

Data collected in the industry tends to relate to accidents and their immediate causes. This may lead to a focus on the most recent serious accident or incident, which may not reflect underlying levels of risk. Safety theory says that, in order to reduce the likelihood of organizational accidents further better indicators of the events and conditions that precede the immediate cause need to be developed and their relationship to underlying levels of risk needs to be determined. I have therefore sought to define a model of risk that would help to develop such indicators. As the railway industry is a large and sprawling system, the conditions that need to be monitored vary from location to location. With this in mind, a set of requirements for an ideal risk model to improve understanding of all of the various causes of accidents and how they combine in a particular situation or location have been developed. In summary, these requirements are:

RMR1: Risk models should allow as many of theevents in an accident sequence to be modelled as is practicable.

RMR2: Risk models should allow as many of the significant and quantifiable technical, operational, organizational and performance conditions that cause accidents or exacerbate risk to be explicitly modelled as is practicable.

RMR3: Risk models should be parameterised by conditions so that the risk at different locations and in different situations on the railway network can be rapidly recalculated.

As safety is ultimately achieved by the actions of safety professionals it is crucial that the models developed by applying this new technique align with the management approaches and actions used in the industry and can be used and understood by decision makers in the industry. Two additional requirements have therefore been proposed on this basis:

SMS1: In order to ensure that they effectively support the management of safety, the uses of a risk models should support the various stages of a safety management system.

SDM1: In order to ensure that they effectively support the taking of safety related decisions risk models should be usable and understandable by those who actually manage safety on the network.

4 Review of industry safety management and risk modelling approaches

I concluded the last chapter by proposing five ideal requirements for risk models to support the management of organizational accidents in the UK railway industry (summarised in section 3.8). In this chapter, risk modelling approaches used in the UK railway industry are described and then reviewed against these ideal requirements.

This chapter presents the argument in support of hypothesis 2: 'Current risk modelling approaches in use in the UK railway industry do not have these characteristics and therefore do not ideally support the effective management of safety.'

4.1 Assessment of the risk of a railway company's train operations.

Railway companies in the UK must undertake suitable and sufficient risk assessment as part of the requirements to receive certification of their SMS by the industry joint economic and safety regulator, the Office of Rail Regulation (ORR). Organisations are legally required to assess the risk of their entire operations as part of a process to ensure that they are doing all that is reasonably practicable to reduce risk.

To support this process RSSB, the industry safety body, has published guidance for train operators to use to undertake risk analysis and assessment (RSSB 2002). The document outlines the principles that should be applied when undertaking risk analysis. For example, this guidance describes requirements for risk analysis which reflect the ideal requirements set out in this thesis, stating that companies must undertake:

'...a detailed [hazard] identification...modified to take account of the specific factors applicable to the operation such as new or different [hazards], causes or consequences and individual potentially high risk locations.' ((RSSB 2002) page 12).

In practice, however, given the scope of their operations and the tools and techniques for risk analysis available to them, it is difficult for train operators to apply these principles in full. In a section describing the choice of assessment methodology the guidance asserts that to produce a 'suitable and sufficient' ((RSSB 2002) page11) risk assessment the train operator should identify:

- The total risk that their operation creates
- The total risk contribution for each hazard
- The total risk contribution of the direct causes of each of these hazards
- The total risk from their train operations to which each type of individual (passenger, member of staff, member of the public) is typically exposed

The identification of the locations or situations on the network where there is the highest risk is not stressed, perhaps because of the inherent difficulties of doing this in practice. One way to estimate the totals bulleted above would be to look at the risk in each location on the network and aggregate it to calculate each total. However this approach is difficult because of the nature of risk on the railway and the practical difficulties inherent in its estimation. Train operations take place over a large geographic area, and the assessment of the risk of each hazard from first principles in each location would be a time-consuming task (as discussed in section 3.6.3). Therefore, train operators tend to apply a 'top down' approach to the estimation of the risk totals. They are able to make estimates of the risk totals bulleted above from the data that they routinely collect for SMIS about incidents and accidents using the risk ranking approach outlined in Appendix B of the guidance (see 2.4.1 for a description of the ranking categories applied). This approach, and the accident causal model that it implies, are summarised in Figure 17.

As has been discussed, to meet the SMIS requirements (see section 3.6.1), companies will tend to record data about accidents and incidents. Incidents like SPAD occurrences or broken rails align with the definition of 'hazards' previously outlined. To assess risk train operators must assess the risk from each hazard. Experts might assess the hazard likelihood by asking: 'how many SPADs occurred on this network in the last five years?' The answer would be considered to provide an indicator of the future likelihood of SPADs occurring. The occurrence rate can then be normalised to a per year figure and used to estimate the likelihood ranking category according to the scheme laid out in Table 1 (shown on page 37). This process might result in a revision to the calculated figure by applying expert judgement to determine how indicative past frequencies are of future likelihood. Similarly the answer to the question: 'What was the average severity of SPAD accidents that occurred over this time period?' could be used to estimate a severity ranking. The risk ranking of this hazard could then be determined from the ranking matrix shown in Table 2. Unlike in the event tree models described in section 2.4.3 the consequence side of the model includes a single accident, representing an accident of average severity. Figure 17 summarises this process and shows how all risk estimates are made on the basis of hazard (incident) data and accident data. No such diagrammatic representation of the causal sequence is produced as part of the process, but the implied causal model is as shown.

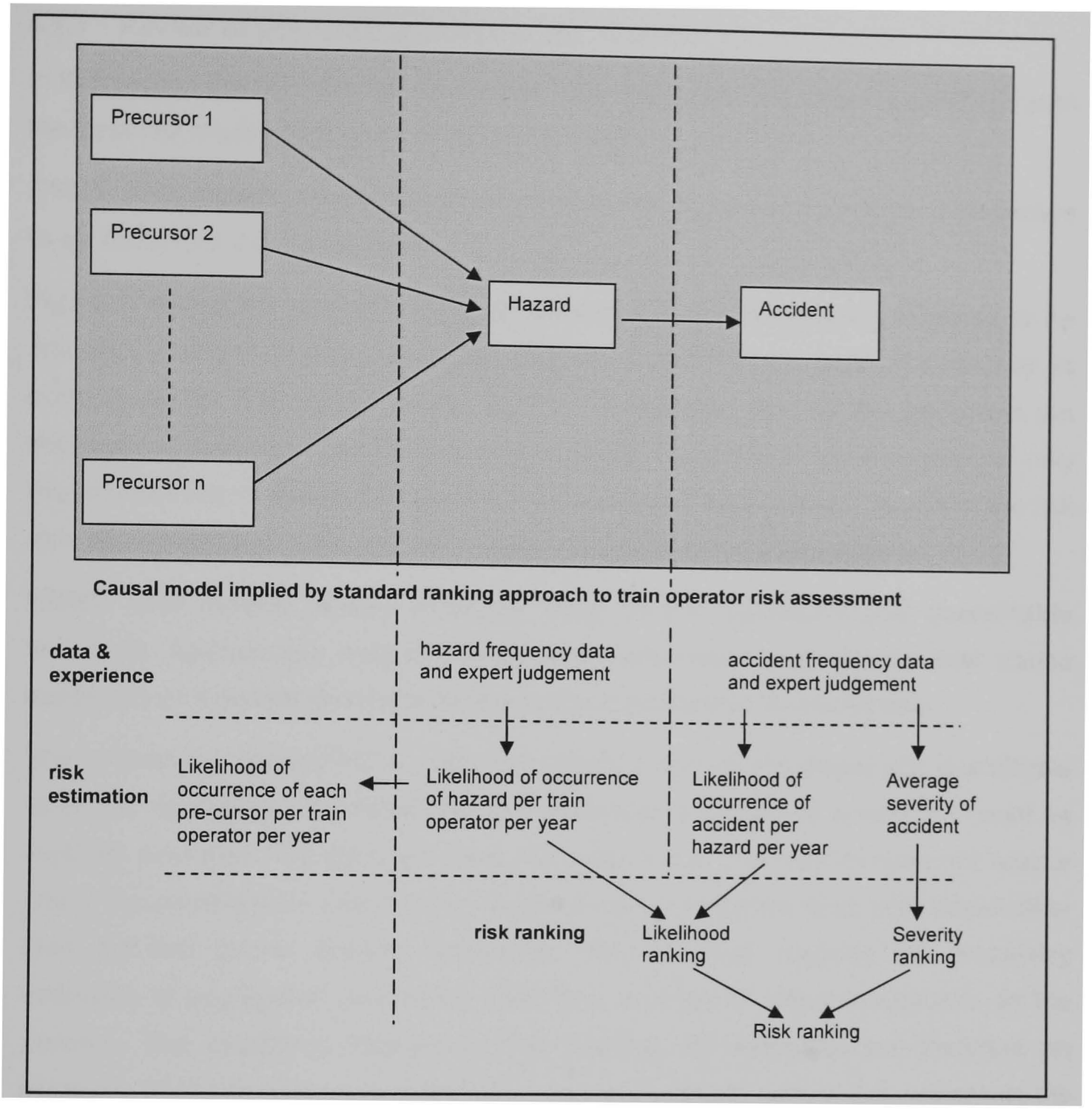


Figure 17: Causal model applied for TOC risk assessment

Note that it consists of only two events: the hazard and the accident. Precursors are not separate events and there is no separate event data to support estimation of their likelihood. The term 'precursor' is used to describe a subset of 'hazardous event' occurrences according to their attributed cause. For example if the hazard was a SPAD, and its attributed cause was a signal failure, one pre-cursor might be 'SPAD due to signal failure'. Another might be 'SPAD due to driver error' etc. Therefore the total SPAD rate would be the aggregate of the rates of all precursors. As was explained in section 3.6.1 there is no requirement in the industry to report data about potential causes of hazards and therefore the model is not at this level of detail. The separate events 'signal failure' and 'driver error', which will only cause SPADs in some circumstances, are not themselves considered.

4.1.1 Review of approach against the risk modelling requirements

In this section the risk ranking approach is reviewed to see the extent to which it meets the ideal risk modelling requirements RMR1-RMR3.

RMR1: Risk models should allow as many of the events in an accident sequence to be modelled as is practicable.

Figure 17 shows the approach does not allow all events in an accident sequence to be modelled. Using the ranking approach there is no model of the accident sequence as such; moreover, the implied causal model is a simplistic one. As the precursors are sub-types of hazard, rather than separate events, the implied model consists of only two events in each accident sequence: the hazard and the accident. Therefore the risk ranking approach enforces a simple model of the accident event sequence.

RMR2: Risk models should allow as many of the significant and quantifiable technical, operational, organizational and performance conditions that cause accidents or exacerbate risk to be explicitly modelled as is practicable.

The second requirement for an ideal risk model is that all significant and quantifiable technical, operational, organizational and performance causes of accidents should be explicitly modelled. The approach does not support this. The method does not require any of the conditions or events in the accident causal sequence to be considered other than the two events already mentioned. The data that supports the probability estimates is aggregated occurrence data from a range of different locations on the network. The conditions relevant to the resulting risk estimates are therefore an amalgam of the conditions in existence in various locations across the network at the time that hazards previously occurred and data was collected.

RMR3: Risk models should be parameterised by conditions so that the risk at different locations and in different situations on the railway network can be rapidly recalculated

Consideration of whether or not risk at different locations and in different situations on the railway network can be rapidly recalculated leads immediately to the conclusion that this is not supported by the process. The analysis is concerned with the total risk to which a train operator is exposed, not the risk in any individual identifiable location.

SMS1: In order to ensure that they effectively support the management of safety, the uses of a risk models should support the various stages of a safety management system

The risk assessment undertaken is intended to impact upon the train operator's safety management system. The guidance document states one purpose of the assessment as being:

'identification of control measures with links to the safety management system...'

The risk estimated relates to the train operator's total scope of operations and the potential uses of the model therefore align with this scope. For example, this approach might be used to justify a proposal that improved driver training procedures are implemented across a TOC's train operations, to reduce SPAD risk. The approach outlined cannot easily be used to identify risk controls that effectively target major train accident risk in particular locations or situations. This is because the approach relies on limited existing data, the weaknesses in the implicit risk model and the lack of conditions and parameterisation in the approach.

However, the approach provides an accessible and easily understandable methodology to help safety professionals consider risk. Therefore even if local issues are not specifically modelled or analysed, application of the method might trigger discussion and local consideration of risk in practice.

SDM1: In order to ensure that they effectively support the taking of safety related decisions risk models should be usable and understandable by those who actually manage safety on the network

Because the approach is relatively simple to apply and understand it is able to be applied by safety professionals and managers within railway companies and supports discussion and consideration of risk issues within companies. However the simplicity of the approach is at the expense of the complexity needed to understand the causal mechanisms that can lead organizational accidents, and the model provides little help for managing safety related to such issues.

Summary

The strength of this approach is its accessibility. To apply the process safety professionals do not need to be expert risk modellers. This is an important advantage of the approach, as it helps to link understanding of risk to the practical management decisions made. The approach therefore partially meets SMS1 and SDM1, in that its use has the potentially to improve the way that an understanding of risk is factored into safety management and decision making.

However, the model is based on a simplified model of the accident event sequence. It does not involve any attempt to model the underlying conditions which increase the

likelihood of events in the accident sequence. Neither does it allow for the particular causes that exist in different locations and situations to be modelled. Therefore it does not provide an approach that is well aligned with the management of organizational accident risk, and does not meet requirements RMR1-3 that were previously proposed.

4.2 The Safety Risk Model (SRM) approach

The Safety Risk Model (SRM) is produced by RSSB on behalf of the UK railway industry. It consists of a series of fault and event tree models representing 125 different hazardous events that have been identified as possible on the UK railway network. It therefore comprises of a set of bow-tie models (section 2.4.4). The SRM is regularly updated by a large team of analysts; the Risk Profile Bulletin (RSSB 2006), which describes the model output, is widely distributed across the industry. The SRM is supported by a database which contains all of the frequency and consequence estimates used as input to the model. A set of model assumptions is also maintained. Figure 18 (taken from (Dennis, Somaiya et al. 2002)) shows a simplified extract from the SRM: a fault and event tree to model derailment risk. The fault tree part of the model is similar to the equivalent part of the model outlined in Figure 17. In general, each hazardous event is disaggregated into the 'precursors' using a number of different base events linked with a large OR gate. As discussed in section 4.1 each precursor relates to a sub-set of the hazardous event occurrences rather than the causal event per se. For example, the model is quantified using data on the occurrence of broken rails which subsequently led to a derailment, not using data on the occurrence of broken rails (see Figure 18).

Each event tree includes a range of different events and outcomes. The severity of the consequences of each accident outcome modelled by the event tree is calculated externally to the model, and then input to the database which provides input data for the model. The SRM is used for estimating the total risk to which the railway industry is exposed from all accidents. It can therefore be used to track progress in the effectiveness of risk and safety management activity in the industry. It has also been used to postulate likely changes in risk associated with network wide initiatives or the update of UK railway standards, which are put into force across the entire network. For example, the model was used to predict the change in risk associated with the widespread adoption of the Train Protection and Warning System (TPWS) as a technical control measure across the UK rail network (RSSB 2003a).

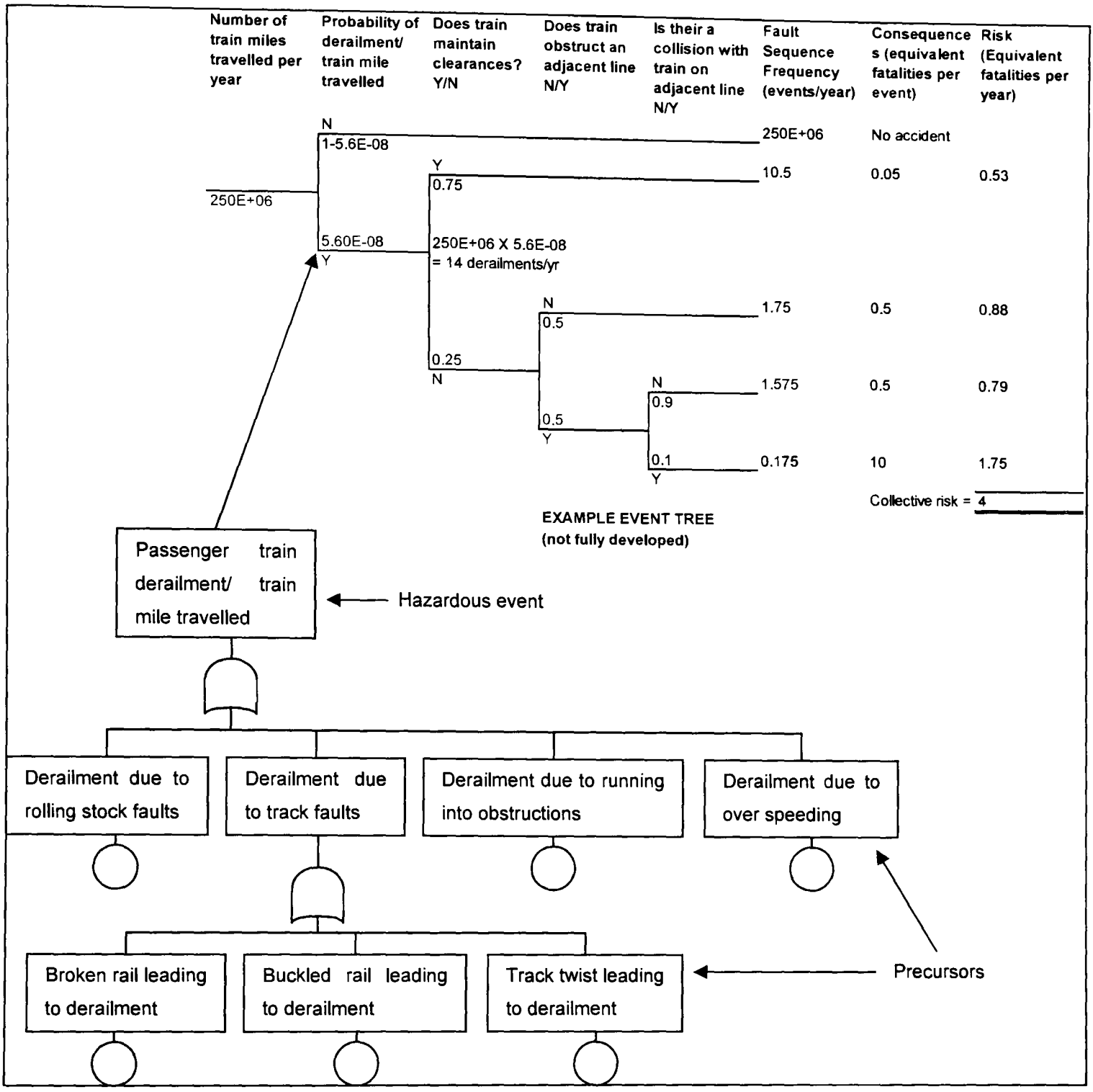


Figure 18: Safety Risk Model (SRM): indicative derailment model

In the SRM Risk Profile Bulletin, risk is defined as:

Equation 2: $risk = frequency \times consequence$

This definition differs from the one presented in section 2.1.1. The SRM estimates the risk across the railway network and it utilises data from across a range of locations and situations to do this. The use of 'frequency' is required in the risk equation rather than 'likelihood' because of this. It is possible that the frequency of each hazardous event type or precursor type across the network could be greater than 1 per year, and therefore this component of the equation is quantified as a frequency not a probability.

To estimate risk the probability of occurrence of possible events in an accident sequence must also be estimated. The past frequency of occurrence of an event is one

indicator of its current likelihood. However, if the circumstances in which a past event occurred are different to the current circumstances then past frequency of occurrence may not be a good indicator of likelihood. Therefore the equation should not be taken to mean that the model produces risk estimates purely on the basis of past event occurrence rates. The term 'frequency' could instead be taken to mean 'estimated future frequency'. The definition shown as Equation 2 should therefore be taken to be a definition which is specific to the SRM, and safety management activities and techniques that make use of it.

Equation 2 provides an indication of the philosophy behind the development of the SRM, for which the preferred method of determining event likelihoods is to use past event occurrence rates. Wherever data is available it is used in the SRM to set the future likelihood of occurrence of events. The Safety Management Information System (SMIS) includes data describing the past frequency of occurrence of hazardous events and hence precursors. Where little data is available, for example when considering low frequency events like train collisions, expert judgement is used to support estimates of likelihood. Judgement is also used to establish whether past event occurrence rates are indicative of the current event likelihood of occurrence. Such judgement might arise when changes to the railway are known to have occurred like the imposition of TPWS and the removal of Mark 1 rolling stock from the network.

As the SRM is quantified using data sourced from across the whole network the model provides an estimate of the total network wide risk. The model breaks down these risk estimates at hazardous event and precursor level. Because of the model's strong reliance on reported industry data it is widely trusted, and used within the railway industry. Its method of development gives confidence that the risk estimates it provides are likely to be reasonable, even for risk allocated at the precursor level. A review of the SRM (Bedford, Quigley et al. 2004a; Bedford, Quigley et al. 2004b) found that 80% of the precursors were within a factor of 10 of the empirical estimates on the basis of judgement. The report suggested that any disagreement was due either to miscalibration of the experts responsible for validating the model or unrepresentative historical data. It proposed further work to address any inaccuracies and improve the model.

4.2.1 Review against the risk modelling requirements

I now consider the degree to which the SRM meets the ideal requirements previously set out for a UK railway risk model.

RMR1: Risk models should allow as many of the events in an accident sequence to be modelled as is practicable.

The Safety Risk Model uses complicated event trees to model the possible sequences of events that follow the occurrence of a hazard. In some of the models, well over a dozen different events are included in event tree models. This aspect of the event sequence is thus well modelled although given its strong reliance on available data, the SRM modelling approach presents a limited model of the causes of a hazard.

A review of the SRM undertaken by the Health and Safety Laboratory (Turner, Keeley et al. 2002) pointed out the lack of depth in the causal model represented by the SRM:

'In general the fault trees within the SRM are expressed at a relatively high level and do not, generally, model the root causes of failures.'

For each incident or accident recorded in the data, it is assumed that there was a single immediate cause, the pre-cursor. For example the data will describe whether a derailment event was caused primarily by a rolling stock fault, or another type of fault such as a track fault, an obstruction or overspeeding. The SRM model only takes account of these immediate causes - the 'active failures' that ultimately triggered the occurrence of the accident. As previously discussed, the precursor is therefore actually a sub-type of the hazardous event rather than a discrete causal event. The other preceding events that organizational accident theory says also lead to its occurrence are not generally recorded in the data and are therefore not generally modelled. In some cases where more detailed incident data is available, for example in the modelling of SPAD risk, the model includes more detailed causal breakdowns.

RMR2: Risk models should allow all significant and quantifiable technical, operational, organizational and performance conditions that cause accidents or exacerbate risk to be explicitly modelled.

The SRM includes a list of assumptions based on knowledge of the states of relevant conditions on the network ((RSSB 2006), Page 70). Most of the assumptions made relate to the event tree part of the model where more detailed information about events and conditions is known and these assumptions are generally made about things like train speed, and the particular characteristics of locations, like tunnels or stations. These are performance conditions and technical conditions, respectively, within the casual taxonomy outlined in section 2.3.1. In general the approach is to assume average condition states rather than specific ones. For example the assumptions state that 'the average speed at which a train will strike a road vehicle at an open [level] crossing (OC) is taken as 10 mph'. Where particular condition states are assumed, this

is done by creating additional instances of the fault and event tree models with revised structure and/or probabilities. For example the derailment model is split into high and low speed models. The SRM assumptions state that the 'the average speed of a fast speed derailment is assumed to be 55 mph'. However, the model does not represent the risk from derailments occurring at 55mph: it represents the network aggregate risk from derailments incidents falling within the set high speed range, the average value of which is 55 mph. Incident data from all incidents arising within the range of speeds is used to produce a new instance of the model.

The SRM model includes some condition states within the model. However these only represent a subset of the condition states of relevance.

RMR3: Risk models should be parameterised by conditions so that the risk at different locations and in different situations on the railway network can be rapidly recalculated

As discussed in the previous paragraph, some models are replicated and different condition states assumed for each part of the SRM. For some parts of the model condition states are introduced as events in the event tree, resulting in sets of event tree end points that relate to different condition states. In the derailment part of the model, for instance, there are separate event tree structures produced for the consequences of derailments occurring at night, at 'peak' times of the day or at 'off peak' times of the day. This is done by introducing an event called 'time of day' into the event tree. The event has three possible states, one for each different time of day modelled, and probabilities are assigned to each state to represent the relative probability that a derailment occurs at each of these times. 'Time of day' is actually an indicator of the performance conditions, 'traffic density' and 'passenger loading'. Given that an accident has occurred, passenger loading is strongly correlated to the severity of the accident consequences, and traffic density impacts on the probability of collision following a derailment.

Building separate models in this way allows the risk from different sets of conditions to be modelled. However, inclusion of multiple conditions states in this way results in rapid growth of model size. By including both high and low speed states the derailment model in effect doubles in size. Inclusion of the three different times of day results in the event tree model becoming three times larger than would otherwise be the case. It is clear to see that it would not take the addition of many more conditions ,or condition states, to make the model unmanageably large. The ultimate implication of this approach is that, in order to build a complete network wide risk model, a separate

model would be needed to represent all different sets of conditions that might occur across the rail network. Currently the model does not contain sufficient parameterisation for it to be used to derive a risk estimate for particular regions of the network. The Health and Safety Laboratory report (Turner, Keeley et al. 2002) concluded that:

'the generic nature of the model makes no allowance for regional differences on the infrastructure'

However, the model is used by train operators to provide an indication of the risk for their particular operations. Each hazardous event in the SRM is associated with a 'normaliser'. For example in Figure 18 the hazardous event is described as 'passenger train derailment/train mile travelled'. Train operators can scale up each normalised risk estimate according to the characteristics of their own operation. RSSB provides tools to support this process[7].

Yet train operators must be aware of the potential inaccuracies in this approach. The normalised figure is not actually representative of the risk at any known location on the network. The model calculates the risk arising in total, divided by the normaliser. This division of the network total figure to a normalised figure is necessary to enable to use of precursor frequency estimates, which may well be greater than 1, to quantify the fault tree model, which is a probabilistic model. A normalised figure (e.g. per train mile) would result in frequencies of occurrence of precursors that are much less than 1. This allows the assumption to be made that the observed frequencies per train mile per year are mathematically equal to probabilities of occurrence per train mile per year.

As was argued in section 3.6.3, risk is not evenly distributed across the network and the total risk on the network is likely to be dominated by the risk in a subset of locations. For example, it cannot be assumed that the scaled risk per track mile relates to a track mile on the network where 'average' condition states (e.g. average train speeds, average track quality, etc) exist. Risk will substantially arise in locations where unfavourable condition states exist in combination. In acknowledgement of this issue the RSSB tools require safety managers to apply their own data to derive risk estimates, wherever possible. The scaled national profile estimates are used only as an indicative estimate of risk where no specific data exists.

---

[7] These tools are not in the public domain, and therefore are not described further in this thesis.

SMS1: In order to ensure that they effectively support the management of safety, the uses of a risk models should support the various stages of a safety management system

As the SRM has a network-wide scope, it provides strong support for safety management at the UK national level. It is used to identify the risk profile of the UK railway network and to provide risk forecasts for the UK railway as a whole. This leads naturally to its use to drive the policy of the railway industry. It is also used to support the development of safety initiatives throughout the industry.

The SRM has been used to estimate the impact of the network wide application of control measures. In 2003, following legislation mandating TPWS fitment, it was used to estimate the risk reduction that would be achieved by implementing TPWS at all junction signals, permanent speed restrictions and buffer stops. The analysis was used to inform a Cost-Benefit Analysis of whether or not installation of TPWS had been justified under the principles of reasonable practicability.

For the reasons already explained use of the model to support local decision making is more difficult and requires additional interpretation and analysis. The CBA analysis mentioned did not attempt to estimate whether it was necessary to install TPWS at a sub-set of locations on the network, perhaps because this would have entailed more extensive remodelling work:

'...no attempt has been made to model degrees of partial fitment.' ((RSSB 2003a) page 32).

Industry safety managers are given access to the RPB presenting the models key findings every time that the model is updated, and also spreadsheets of the risk estimates broken down by hazardous event and pre-cursor. This allows them to extract risk estimates from the SRM for the purposes of their own calculation and assessment. However their estimates do not relate to their particular scope of operations so it can be difficult for them to extract such information. There is a paucity of data at the local level and the SRM provides a start point to assess if they think they are above or below the network risk level reported in the SRM.

The model therefore supports policy and planning well at the network level. It is also strongly linked to the incident data via SMIS and is clearly well integrated with industry monitoring activity. For particular safety managers, use of the SRM to support their own safety management activity is more problematic requiring a degree of interpretation, and an awareness that in some cases SRM output may not be useful or relevant.

SDM1: In order to ensure that they effectively support the taking of safety related decisions risk models should be usable and understandable by those who actually manage safety on the network

The Safety Risk Model provides the industry with estimates of the average risk for a wide number of hazards, and precursors across the railway network. These estimates are strongly driven by data collected, and are developed by a robust and trusted process. This gives the industry confidence in their validity, and helps to ensure that they are used in practice. The data is most useful for control measures with a wide scope of implementation, where the average risk estimates provided are most likely to be valid.

As previously discussed, the risk estimates are less useful for decision making relating to specific situations or locations as the SRM scope will not be aligned to such situations. In these circumstances the analyst will require a detailed understanding of the assumptions of the model, and these are not fully transparent. Work is under way to develop detailed definitions of the meaning and scope of hazardous events and precursors, to make the underlying assumptions of the model more transparent to its users. However, the underlying fault and event trees on which the risk estimates for the major accidents in the model are based are not routinely made available to industry safety managers so they are unable to examine and review these models to ascertain their validity in particular circumstances, and in any case competence in risk modelling would be required to do so. Without such understanding the models might be misunderstood and misused.

Summary

The SRM is a substantial and trusted model in the industry with many uses, particularly with regard to national policy, planning and initiatives. For this reason, when considered within its intended scope, the model substantially meets requirements SMS1 and SDM1.

However, the model was not developed specifically to support the management of organizational accident risk and does not meet all of the requirements outlined for such models. From this perspective it only partially meets requirements SMS1 and SDM1 as the models network wide scope means that a detailed understanding of its scope and assumptions would be needed to truly understand how the risk estimates it provides translate to the local level. This understanding is hindered in particular by the fact that the fault and event tree parts of the model are not available to the users of risk information.

The SRM partially meets RMR1. The event tree side of the model includes detailed analysis of the sequences of events that could result in an accident, following the occurrence of a 'hazardous event'. However the fault tree side of the model describes only a single measurable event. The model does not meet RMR2 as it contains a limited degree of parameterisation by condition, and the approach to inclusion of conditions – duplication of the model structure – does not provide a viable way of extending parameterisation to a significant degree. Because of this limited degree of parameterisation the model does not meet RMR3. Scaling the national aggregate risk by a normaliser would not support the identification of 'risk hotspots' as by definition the estimate represents average risk rather than a possible upper estimate.

4.3 Quantitative risk assessments – industry study

Safety approvals or justifications are usually required to allow changes to be made and a risk assessment will often form the basis of an argument presented in a technical report, or a safety case, to argue that the adoption of a new system or procedure is justified. This is implicitly acknowledged in the industry safety management guidance the Yellow Book (RSSB 2007b) which is scoped to address 'engineering change'.

Because of this focus on justification of change, and the considerable effort and expertise needed to build risk models, individual organisations in the UK railway industry do not maintain their own risk models for all accidents to which they are exposed. Instead, they tend to undertake bespoke risk assessment and modelling on a case by case basis. Organisations may wish to undertake risk modelling to:

- Determine whether a new system can be safety installed, and how to do this most safely. This could range from the installation of closed circuit television at a station to the introduction of a new signalling control centre.
- Determine whether alterations to procedures can be safely undertaken, and how to do this most safely.

By definition, these bespoke assessments are limited in scope to consider only the possible effects of each intervention.

Next one particular analysis is considered, as an example of how this approach is applied. Section 4.3.1 is based on insights into the strengths and weaknesses of the modelling approach that were gained by a review of the analysis, and resulting model with its original author. Note that the study is subsequently used as the basis for the core modelling work of this thesis which is described in Chapters 7 and 8.

4.3.1 Urban derailment risk analysis

A 'derailment study' (Howes 2001) was carried out as part of development studies for a proposed upgrade to an urban railway.

The objective of the original study was to quantify the level of risk to passengers and staff arising from derailments on the railway and use this information to undertake the upgrade in the optimum way, ensuring that risk was reduced to as low a level as was reasonably practicable. Fault and event tree models were used to calculate the risk from a number of different consequences that could occur following derailment. The analyst decided that the risk assessment should comprise of six different fault and event tree models, each representing a distinct type of location on the network. The models were developed from the structure of an early version of the SRM. Therefore the fault tree side of each model consisted of the hazard 'train derailment' and a range of precursors. The event tree part of each model was more elaborate, consisting of a range of different events that could occur following the occurrence of the hazard. The process followed for the development of these models is broadly the same as that applied to develop the SRM. The set of event trees produced as part of the model are shown in Appendix A1. The event tree for a twin track tunnel is shown below.

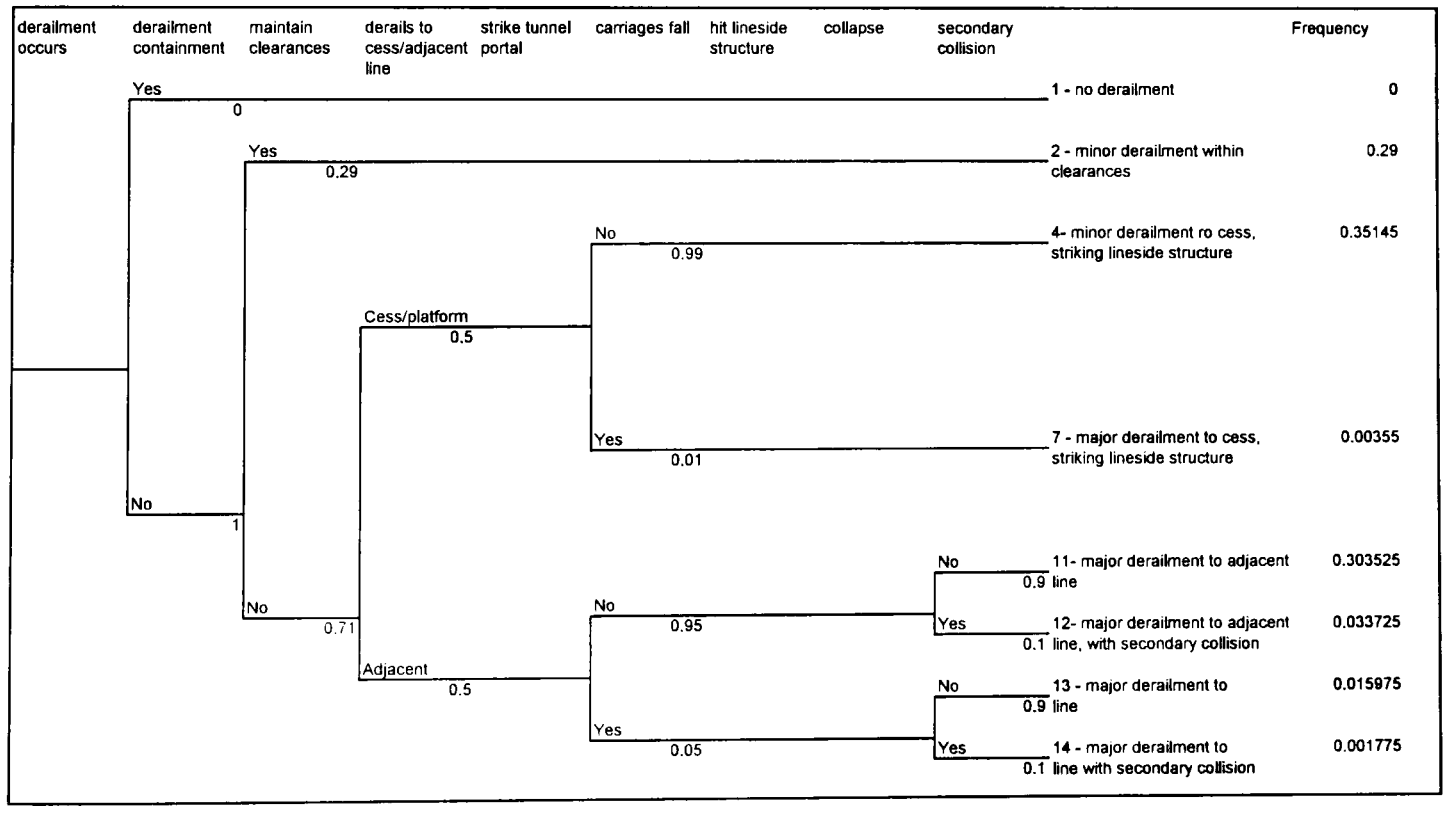


Figure 19: Twin track tunnel on a section of urban commuter railway

Table 3 describes the meaning of each of the events in the set of event trees for the study. In order to support the work described in this thesis (some time after the analysis had been undertaken), the assumptions under which the event trees were produced were reviewed with the risk analyst who had initially developed it (see appendix A2).

This provided an opportunity to investigate how effectively the condition states that form the underlying assumptions of the models had been documented, managed and accounted for in this risk analysis.

Condition	Condition description
location of derailment	the location where the derailment occurs
derailment containment fitted	whether the derailment containment is fitted.
track curvature	the curvature of the track
number of tracks	the number of adjacent tracks:
track type	whether or not the track is predominantly plain line or whether it contains switch and crossing
train speed	the speed of the train when derailing (mph)
lineside object density	the density of objects beside the line
lineside object type	the type of equipment beside the line
Density of traffic	the traffic density
rolling stock type	the type of rolling stock

Table 3: Conditions whose state affects fault and event probabilities

4.3.2 Review against the risk modelling requirements

I now consider the extent to which the modelling approach outlined meets the ideal risk modelling requirements that were set out in section 3.8.

RMR1: Risk models should allow as many of the events in an accident sequence to be modelled as is practicable.

The modelling approach undertaken is based on the structure of the SRM. Therefore the event sequence is modelled in a similar way. A detailed sequence of events is included in the event tree, however the fault tree part of the model is simplistic modelling only one event - the hazard itself.

RMR2: Risk models should allow as many of the significant and quantifiable technical, operational, organizational and performance conditions that cause accidents or exacerbate risk to be explicitly modelled as is practicable.

The analyst was asked to identify the conditions which he believed he needed to know in order to estimate the probability of occurrence of each of the events in the model. Table 4 shows the conditions that the analyst identified, and the events to which they relate.

Event	Event Description	Relevant conditions
Derailment occurs	The train derails (top event of the fault tree)	Track type Track condition Track curvature
derailment containment	A raised containment rail is present, which contains the derailment by limiting the sideways movement of the train.	Derailment containment fitted Train speed
maintain clearances	Following derailment the train remains clear of any obstruction. It does not overlap adjacent lines or obtrude beyond the edge of the track area.	Track curvature Train speed
derails to cess/adjacent line	The train can derail to either side of the track. Derailing to the 'cess' (the outside edge of the track area) may lead to a collision with a structure beside the railway line. Derailing to the adjacent side may lead to a collision with another train.	Number of tracks Train speed Location of derailment
carriages fall	The carriage does not remain upright.	Train speed Rolling stock type
hit lineside structure	The train hits a structure beside the line, such as a station platform or a building.	Location of derailment Train speed Lineside object density
structure collapse	Collision with a structure causes the rolling stock carriage to collapse or break apart.	Train speed Rolling stock type Lineside object type
secondary collision	The derailed train collides with a following or on-coming train.	Density of traffic

Table 4: Events and the conditions whose state influences their likelihood

The analyst was subsequently asked to identify the set of these condition states that formed the underlying assumptions of each of the six models produced during the study. The sets of conditions identified are shown in Table 5.

In some cases, the same assumption was made for all six models. For example, it was assumed that all traffic on this section of the network consisted of electric multiple units (EMUs) and it was assumed that the track had 'severe' curvature throughout. In other cases, specific condition states were assumed for specific types of location.

	Model 1	Model 2	Model 3	Model 4	Model 5	Model 6
Location	Open track	Bridge	Stopping Station	Tunnel	Through station	Tunnel approach
Containment	No					
Curvature	Severe					
Tracks	4	2	2	2	2	2
Track Type	Plain line & S&C	Plain line	Plain line	Plain line & S&C	Plain line	Plain line & S&C
Train Speed	30mph	30mph	<15mph	30mph	30mph	30mph
Lineside Object Density	High	N/A	High	High	High	High
Lineside Object Type	Anchored	N/A	Anchored	Anchored	Anchored	Anchored
Density of Traffic	High					
Rolling Stock Type	Electric Multiple Unit (EMU)					

Table 5: Condition states assumed for each of the six fault and event tree models

For example, the train speed is only less than 15mph in stations where the train is scheduled to stop. All of the conditions relate to the event tree part of the model except 'track type' which relates to the fault tree part of the model. The 'open track', 'stopping station' and 'tunnel approach' models include precursors to model both switch and crossing (S&C) faults and plain line faults, whereas the other models include only 'plain line' faults.

The analyst found it quite easy to derive the condition states shown in Table 5 despite the fact that the analysis had been undertaken nearly four years previously. However despite this a review of the assumptions described in the report found that the assumptions that the analyst identified in the exercise were not completely and consistently described in the report.

As has previously been discussed, fault and event trees describe failures and events. They do not support the explicit modelling of the underlying conditions or their states. Therefore these conditions must be documented separately in any report supporting an assessment. The report is very thorough in this area, with a section used to describe the underlying assumptions in detail. Nevertheless there are some assumptions which are not documented in it. For example:

1. The report does not state the assumptions made about the number of tracks in each location.

2. The report states that only one train speed would be assumed for the models – an average speed of 30mph. It is not stated that the train speed in stopping stations will be lower than this.

In the case of 1 above, the models provide some implicit information that a thorough reviewer might be able to use to deduce the assumption. Review of the event 'derails to cess/adjacent line' in event trees 2-6 shows a 50% chance of derailing in either direction which indicates the presence of a twin track layout. In event tree 1 there is a much higher probability of derailing towards an adjacent line which could be assumed to imply a larger number of tracks.

In the case of 2 above, Table 4 shows that there are a number of events that the analyst identified as being affected by speed. The probabilities of occurrence of all of these events differ in the 'stopping station' model when compared with the probabilities of occurrence in other event trees. The analyst had therefore diligently considered the impact of this change in speed despite the fact that this difference was not explicitly documented in the model or as an assumption. Nevertheless, as this discrepancy had not been documented, anyone analysing the results of the report or trying to re-use its structure for another application would have to infer this difference in speed.

Ensuring the correct recording of condition states as assumptions of the analysis, is only the first problem to be addressed. Having clarified exactly what the assumptions underpinning the analysis were, it is then possible to investigate whether they were logical and supportable. In some cases, the assumptions did not appear sound. For example, the report states that a speed of 30mph is assumed across the analysis but elsewhere in the report it is assumed, on the basis of past experience that derailments occur at an average speed of 42mph, so this speed is used to calculate the severity of derailments. Speed is therefore modelled inconsistently in different places in the model. The past evidence indicates that trains that derail tend to do so at a higher speed than the average across the network. This disparity in average train speeds and average derailment speeds highlights a key problem with the use of average values as assumptions in the analysis. Using an average value as an assumption neglects the fact that accidents are most likely to occur in 'risk hotspots' where undesirable condition states are coincident. The accident is more likely to occur where there is high speed and severe track curvature than where there is 'average' speed and 'average' track curvature. The use of an average value therefore underestimates the level of risk

in certain locations. In other parts of the model extreme values are used, rather than averages. The problem with this approach is that it creates a mismatch between the assumptions and reality. Worst case conditions will, by definition, only arise in certain locations on the network. The risk will be at its highest in these locations.

RMR3: Risk models should be parameterised by conditions so that the risk at different locations and in different situations on the railway network can be rapidly recalculated

The major assumption made in the analysis is that any location on the network can be represented by one of the six models. By extension, this means that only the six sets of conditions outlined Table 5 exist on the network analysed.

Investigation of the condition 'track curvature' shows that this assumption is a gross simplification. For this condition, the analyst did not use an average. Instead he made a worst case assumption that track curvature is 'severe' across the whole of the infrastructure area modelled. The analyst confirmed that only up to 80% of the network is either 'severely' or 'moderately' curved, with the remaining 20% being straight track. The likelihood of certain types of derailment is strongly correlated to the degree of track curvature. If it is assumed that all track curvature is severe then the risk estimated by the model for moderately curved or straight track on the network is likely to be an overestimate. In turn the risk estimate for track that is actually severely curved is likely to be an underestimate. A similar principle applies when making the assumption that traffic density is always 'high', when in fact it varies significantly. Most of the risk on the network will actually relate to the locations where track curvature is severe and traffic density high. In locations where track is straight and traffic density low, the risk will be much lower. However, the models do not have sufficient resolution to distinguish between locations where these differing condition states exist.

In the SRM separate event trees were built to take account of the differing states of the conditions train speed and traffic density in the estimation of outcome severities. I previously argued that, to enable risk estimates to be made under these conditions, similar duplication of fault trees would be necessary. Following this approach three separate versions of each model would have been needed to take account of the variation in track curvature described by the risk analyst: the first assuming 'severe' curvature, the second assuming 'moderate' curvature, and the third 'no curvature'. This would have resulted in eighteen separate models being produced rather than the six that were actually built. If the model was then expanded to include two possible condition states for 'traffic density', 36 separate models would be needed. Extending

the model to account for a wider variation of conditions states to produce a higher resolution of model results in an exponential increase in the size of the model produced. It is therefore clear to see why this approach is not followed. The larger the model, the more difficult it is to manage and the more time-consuming it is to produce. Therefore an analyst must use their judgement to select a representative set of models for a particular problem. In this case, the analyst made what appears a sensible judgement from the perspective of manageability in restricting the analysis to six separate models. However, the fact that gross simplifications were needed in the model assumptions to do this illustrates that there are flaws with the current approach to the application of fault and event trees to risk analysis in the UK railway industry.

SMS1: In order to ensure that they effectively support the management of safety, the uses of a risk model should support the various stages of a safety management system

In this study, the risk model is used support the planning stage of the Safety Management System. The model is not location specific. It looks at risk across the core derailment study area.

Risk assessment is undertaken in order to argue that the risk is reduced to as low a level as is possible. The report investigates whether particular control measures, like the installation of containment rails, will have an impact on derailment risk.

SDM1: In order to ensure that they effectively support the taking of safety related decisions risk models should be usable and understandable by those who actually manage safety on the network

The approach meets SDM more fully than the SRM, as it is a bespoke model produced for a particular project. The insights gained by undertaking the modelling approach would be made by analysts within the project, and therefore it is possible that these insights would inform any risk based decisions made.

Summary

The model fails to fully meet RMR1 as the fault tree part of the model is simplistic models only one event. It also fails to substantially meet RMR2. Condition states are not modelled in fault and event tree analysis. The condition states that form the assumptions of the model are instead documented in the supporting report. However in the particular study that I investigated not all condition states were documented. This makes inconsistent assumptions more likely. For example, in this study two different and inconsistent assumptions were made about train speed. Conditions can easily be

ignored or overlooked. In certain circumstances it may be considered self evident that a condition exists, and therefore consciously or by omission it is not documented. But the state of such conditions may change. They can differ from location to location, or change gradually over time. Failure to thoroughly document conditions can make it harder for others to understand and interpret the results of an analysis. It also makes it easier for the state of conditions to be set inconsistently in an analysis. In summary, the documenting and management of conditions is a complex task. They are generally considered as assumptions of any analysis, and the review highlights that there is currently little or no methodological support to help analysts consistently record and manage them.

The model also fails to meet RMR3 as it is not parameterised. Six separate models are produced, each assuming a different set of condition states. However many more sets of conditions than this are likely to exist across the railway network under analysis. Unfortunately the inclusion of more conditions states in the model using the fault and event tree approach would lead to an exponential increase in the number of models required and is not practically possible.

The approach partially meets requirements SMS1 and SDM1 as it supports planning decisions on a project and the application of the modelling process itself would help to educate the organisation responsible for taking any related decision.

4.4 Chapter summary

In this chapter, the extent to which UK railway approaches to risk assessment and modelling meet the ideal requirements that were previously proposed were reviewed. By reviewing the ways in which risk is modelled in the UK railway industry, against requirements derived in Chapter 3 it was found that none of the approaches has the ideal characteristics to support organizational accident risk modelling that were outlined in section 3.7. Therefore the chapter provides the argument in support of hypothesis 3. In particular:

- No current models allow all of the causes of accidents, both events and conditions, to be explicitly modelled (RMR1, RMR2).
- None of the models or techniques identified is parameterised. Therefore none could be used to rapidly analyse risk in different locations and identify possible risk hotspots (RMR3).
- Each approach has limitations in its use to support safety management activities and the taking of safety related decisions (SMS1, SDM1).

Although none of the models are parameterised by condition information, both the SRM and the industry bespoke risk model included some duplication of fault and event trees. This acknowledges the need to model risk under different circumstances and provides support for the validity of requirement RMR3.

The risk assessment and modelling approaches are strongly linked to the availability of data and therefore these models are based on truncated models of the event sequence and fail to include underlying conditions. None of the approaches reviewed fully met any of the modelling requirements RMR1-RMR3.

5 Review of related risk modelling approaches and research

In this chapter I review risk modelling approaches and research which indicate how models that meet the ideal requirements of Hypothesis 1 (outlined in section 3.8) might be developed. None of approaches fully meets these ideal requirements, although each provides some insight into what a new approach might look like.

5.1 General

Research has been undertaken to look at modelling of certain types of railway risk. For example, Podolfillini et al (Podofillini, Zio et al. 2006) describe a model for optimising railway track inspection to improve reliability and maintenance. The research is based on the detailed analysis of the results of ultrasonic rail inspection cars, and uses a simple barrier model of cause, rather than a more detailed analysis of the possible accident event sequence. Neural network have been used to estimate how earthquakes might affect train acceleration at a range of stations on the Taiwan high speed rail system (Kerh and Ting 2005). Their work identified one station which potentially had much higher risk than all others on the line.

However there is much less work which tries to develop new or improved generic approaches or extensions to existing standard risk modelling techniques that could potentially meet the ideal modelling requirements outlined in this thesis. In sections 5.2 to 5.5 the research in the area of risk modelling with the most relevance to this thesis is described.

5.2 The Irish Rail risk model

Sotera Risk Solutions has developed a risk model for Irish Rail that can estimate the variability in risk from location to location across the Irish rail network (Sotera 2007). All significant hazards occurring on the Irish railway network were modelled using fault and event trees. The logic for each of the hazards was initially developed using standard fault and event tree software. In order for the model to quantify the risk in each location, each of the failures and events in the model for each of the hazards were parameterised, so that the failure rates and event probabilities depended upon the details of the asset design and condition in each location and the usage of the system by trains and passengers. It was then necessary to obtain all the indicator data to populate the model. This was achieved by linking to the operators asset databases which hold the relevant information on asset design and condition, and taking information from timetables, level crossing use, passenger counts and so on. Despite this, Sotera encountered problems with the availability of data to quantify their model

and therefore supplemented available data with expert judgement to quantify their model. The model focuses on known differences in railway assets and performance. In other words, it considers physical differences rather than operational or organizational ones. The parameterisation of the model is undertaken in an additional layer of software.

The model has many of the attributes that I have argued are necessary. It incorporates a low level of causal analysis in its fault trees and a long sequence of events in its event tree models and therefore substantially meets requirement RMR1. It also includes a range of technical and operational conditions. Some time-varying conditions are included in the model, such as asset condition, passenger loadings, and rail traffic levels. However, the model does not include operational or organizational conditions which would also be expected to vary over time. It would be difficult for Sotera to expand the model to include operational and organizational conditions using fault and event tree techniques for the reasons that were outlined in section 2.4.2. It therefore partially meets the requirements that were set out in RMR 2.

The model is parameterised to include technical conditions and performance conditions, in addition to failures and events (substantially meeting RMR3). But, there is a limit to the degree of parameterisation that can be applied to the model. The Irish railway network is broken down into 227 specific locations, where it is assumed that specific sets of conditions exist. In practice, a location is either a station area or a section of infrastructure typically 5km long. The model therefore assumes that there is no variability in the states of conditions in each of these areas or track sections. In effect this is the same approach as was used in the industry study (section 4.3) although that used only 6 different sets of trees and so did not select the condition sets modelled in such a systematic or considered way.

Irish Rail has recognised the need to build models which capture specific assumptions so that risk form high risk locations on a railway network can be estimated. This work therefore provides support for the validity of the risk modelling requirements outlined in this thesis.

The uses of the Sotera model reflect its focus on technical and performance conditions, for example the model has been used to look at the benefits of redeploying existing assets; a significant reduction in network risk was achieved by deploying rolling stock differently across the network since it was found that the least crashworthy trains were used on the lines with the highest potential for an accident. Particularly acute high-risk locations and assets have also been identified (e.g., lightly used lines which, given their

configuration and the condition of assets, present a high level of individual risk). It would be difficult for Sotera to expand the model to include operational and organizational conditions using fault and event tree techniques for the reasons that were outlined in section 2.4.2. The model is able to estimate network wide risk, as the additional software is used to aggregate the risk in all locations to a network-wide total.

However, there is one key drawback to the model, when considering its uses to support safety decision making (SDM1). As the parameterisation is handled in a separate layer of software the model is a 'black box' and the fault and event tree logic is not visible to the user. When local risk figures are calculated, the model also fails to provide updated fault and event tree models of the relevant accident causal sequence. This will therefore limit the extent to which local decision makers would be able to use and interpret the results.

5.3 RSSB/Risk Solutions derailment risk model

The UK railway industry has recognised that risk models which include both events and conditions, and which can be used to model risk in specific locations are potentially useful. RSSB commissioned research to consider: *'the feasibility of developing a risk model capable of describing the complex interactions that create and mitigate the derailment risk due to track faults.'* (Campbell and Kennedy 2003).

The research suggested that if it were possible to build such models they would help to understand the true levels of risk at specific locations or at locations with common characteristics. This would then allow the model to be used to help determine the effect of asset condition, or different control strategies on risk.

The researchers investigated a number of different ways of building their model and finally settled on an approach using a traditional fault and event tree, supported by an additional fault tree which modelled condition states. Condition states were referred to as 'environmental factors' and this second set of fault trees was called the 'environment module'. The 'environment module' fault trees were used to calculate the probability of occurrence of different possible combinations of condition states. A layer of software was used to link all the models. A 'fault module' was developed to calculate fault tree base event probabilities given different combinations of environmental conditions. Similarly the 'consequence module' calculated the probabilities of events in the event tree given the different combinations of condition states.

As was discussed in section 3.6.1, the industry does not have a complete set of data and asset records which describe the combinations of condition state in each and

every location on the network. Therefore the probability of condition states was estimated from their total network incidence. For example, using network data the modellers estimated that 2% of the UK railway network consisted of track in tunnels ((Campbell and Kennedy 2003), p95). Estimation of network wide populations in this way provides no model of how different sets of locations combine in particular locations. To model this an influence diagram was developed. This modelled the strength of conditional probability relationships between environmental factors, and hence which condition states were more likely to be coincident in particular locations. The model included eleven different environmental factors, each with three to six separate states. The influence diagram is shown in Figure 20. Broken arrows are used to denote weak influential relationships; solid arrows denote strong relationships.

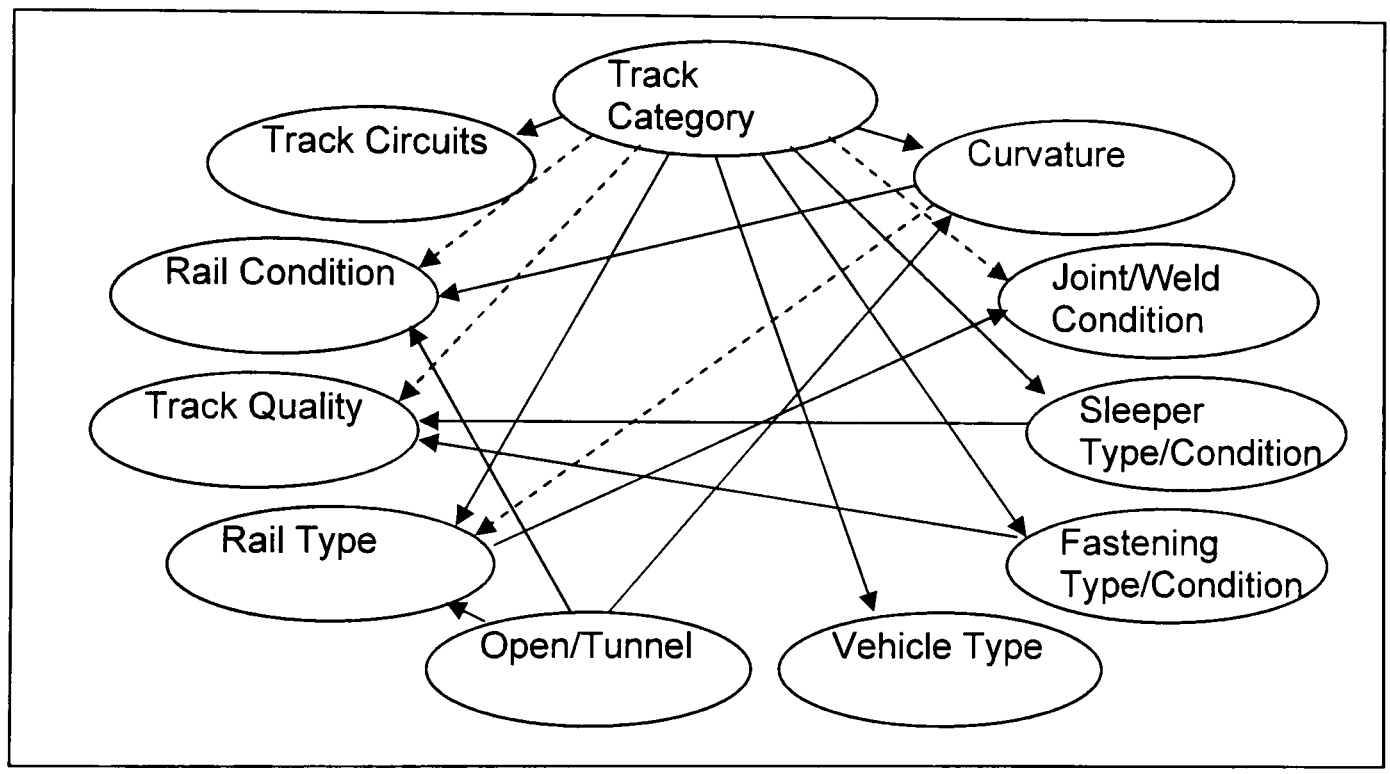


Figure 20: Environmental factors influence diagram

The study identified nine separate track faults that should be modelled with separate sets of fault trees and only one, 'gauge spreading', was built in earnest. Not all condition states were included in the environment module. Separate fault tree structures were used to model high, medium and low severity gauge spreading. Also separate trees were built for low and high speed operation

The conceptual model was built and indicative output results obtained. However the model was never developed beyond its initial phase. The research report does not provide any explanation of why the work was not taken forward. The most likely explanation for this is that the model produced was too large as to be of practical use. As conditions and faults were each being modelled using fault tree techniques, the same exponential increase in model size that was discussed in 4.2.1 and 4.3.2 was

evident. This problem was lessened to an extent by the use of two separate fault trees. However even with the selection of a small scope of model focussing on derailment due to gauge spread for the purposes of demonstrating the approach, the degree of parameterisation modelled resulted in significant repetition of fault tree logical structures, and hence a large and unwieldy model. A large section of the research report is taken up simply with documenting the fault trees produced.

Were it possible to develop this model, it may have met requirements RMR1-RMR3 more fully that the existing techniques were reviewed in Chapter 4. The model includes a more complex model of the event sequence than the existing industry approaches previously investigated as the fault trees are developed to several levels of abstraction. The extract of the fault tree part of the model shown in Figure 6 shows a portion of the model with a number of separate base events, and this is a small sub-set of the total fault tree model. A number of condition states are explicitly modelled. Some are embedded in the fault tree model; others are explicitly modelled in the 'environment module'. The model includes detailed and explicit modelling of over a dozen different condition states, and could be used to calculate the risk with all possible combinations of them. Unfortunately the approach suffers from the practical difficulties associated with building and maintaining models with such a high degree of parameterisation. A model of this type that included enough of the individual causes of risk to be useful would be too large to build, maintain and use.

Nevertheless this research provides further validation of the hypothesis that these types of model are desirable as there is clearly an interest in the UK railway industry in their development. The research also provides evidence of the difficulties of developing parameterised models using fault and event trees that were previously outlined in sections 4.2.1 and 4.3.2.

5.4 LPSA and risk monitors

Similar requirements to those that were set out for ideal risk models in the railway industry have driven the development of tools and techniques in other industries. Following the Three Mile Island nuclear accident in the US, there was recognition that the traditional focus of accident prevention on the design of nuclear power stations, and the inclusion of a high degree of redundancy in the system functions needed to change (Joksimovich 1994). This led to a focus on risk models which were able to be used to predict and monitor the variability in conditions that might arise throughout the operational life of nuclear power stations such as changes in plant configuration, operational procedures, repair and maintenance activities and aging of equipment and

components. This approach is called living probabilistic safety assessment (LPSA) and is defined by the IAEA as:

'a PSA of the plant, which is updated as necessary to reflect the current design and operational features, and is documented in such a way that each aspect of the model can be directly related to existing plant information, plant documentation or the analysts' assumptions in the absence of such information.' (IAEA 1999) p1).

A living PSA builds on standard risk modelling approaches like fault and event trees. It extends these techniques to model underlying assumptions explicitly and link these directly to known information and data about the system. This approach reaches its logical conclusion with the use of LPSA to supports the use of Risk Monitors which are defined by the IAEA as:

'a plant specific real-time analysis tool used to determine the instantaneous risk based on the actual status of the systems and components. At any given time, the safety monitor reflects the current plant configuration in terms of the known status of the various systems and/or components, e.g. whether there are any components out of service for maintenance or tests. The safety monitor model is based on, and is consistent with, the LPSA. It is updated with the same frequency as the LPSA. The safety monitor is used by the plant staff in support of operational decisions.' ((IAEA 1999) pp1).

The relationship between living PSA and risk monitors is clearly described in the forward to CSNI technical papers number 7 and 8 ((CSNI 2004) page7):

'The aim of the risk monitor is to provide an estimate of the point-in-time risk for the current plant configuration and environmental factors whereas the LPSA provides an estimate of the average risk hence uses average initiating event frequencies and maintenance unavailabilities and usually takes account of the exposure time to different initiating events as the plant passes through the different plant operational states modelled in the PSA. Hence, the LPSA model needs to be reviewed for any average or assumed conditions in the model to ensure that an accurate point-in time risk is calculated for all configurations.'

Tools like RiskVu (Pullen 2002) can be used to develop living PSA models and risk monitors. Risk Vu provides a high level interface to fault and event trees built using *Fault Tree+* (Isograph 2007). The models consist of Master Logic Diagrams and Event Sequence Diagrams. A Master Logic Diagram is essentially a generic fault tree models which describes the 'top logic' (i.e. the full set of fault sequences that the system might experience given the range of system operating parameters). An Event Sequence

Diagram shows a sequence of events and their potential outcomes. These outcomes are those events which occur after an initiating event, leading up to end states and consequences. It is similar to an Event Tree, but is used in more advanced risk assessment methodologies where the modelling of event sequences needs to be more flexible.

The interface consists of a model of the system, for example the particular nuclear power plant, in which various parameters can be changed and used to update the underlying fault and event trees.

The philosophy behind the use of living PSA and risk monitors is very similar to the philosophy and approach to risk modelling that I have argued should be applied in the railway industry. Kafka explains that:

'If [systems] were managed so that critical high-risk configurations and actions did not occur, then risk would be small and practically no severe accidents would occur' ((Kafka 1997) page 198).

These 'high-risk configurations and actions' describe the conditions whose existence would indicate an increased risk of organizational accidents. The concept of the risk monitor in the nuclear industry finds its parallel in our stated requirement for a location specific risk model. The risk monitor is used to capture a snapshot of the system in time and the risk estimate given the relevant parameters. I argue that in the railway industry uncertainty in risk estimates comes primarily from the inability to capture variation from location to location across the network. Therefore risk snapshots in the UK railway industry should reflect particular locations and performance parameters.

Despite the similarities in philosophy, the location specific nature of a proposed railway model means that it would not be a simple matter to apply this technique to produce the ideal model. The proposed railway model would have the potential to model risk in a range of locations across a very large geographic scope. Given the scale of the model it is not anticipated that causes should be modelled to the level of abstraction implied by the use of system models to capture parameter changes. The use of system models means that the technique focuses on classical reliability parameters. In this thesis the focus is on the key technical, operational and organizational conditions of the entire railway system and their causal relationships, rather than on developing a model of the railway system function itself, which would be highly complex.

The existence of LPSA and Risk Monitors in other industries which are prone to organizational accidents again provides some support for the argument that similar models should be developed for the railway industry. The prime concern of LPSA is

temporal change in the parameters that cause risk. In the UK railway industry there should be additional concerns relating to the variability from location to location across a large rail network.

5.5 Improving probability estimates from a limited data set

(Quigley, Bedford et al. 2007) have undertaken research into how to improve the probability estimates used within the SRM. They note that many of the SRM precursors are rare events. In these instances, estimation of precursor probability (by calculating the ratio of the number of events that have occurred to the period of observation), is prone to inaccuracy. In particular, there is a high probability of zero estimates, when no events are observed; limited observations also result in huge differences in probability estimates. They advocate the use of Empirical Bayes techniques, which use pooled data rather than subjective estimation, to improve probability estimates. Precursor data is pooled to estimate an overall rate of occurrence, and then adjustments are made from the pooled rate for each individual event. Essentially certain statistical parameters can be inferred from the pooled data set and used to inform the estimation of individual pre-cursor probabilities. The work has been taken forward by RSSB and is used to improve probability estimates in the SRM. The authors acknowledge some potential weaknesses to the approach, in particular in identifying a set of precursors to be pooled together with broadly similar occurrence rates.

This research was undertaken in response to the data problem outlined in section 3.6.1. It takes as its starting point the assumption that the data set is limited to the recorded numbers of occurrence of each pre-cursor in the SRM. The solution advocated here is to obtain more detailed understanding of events preceding the occurrence of each precursor and conditions which are correlated to its occurrence.

The two approaches are therefore not mutually exclusive. The approach advocated here places an even greater reliance on the availability of data than the SRM. The Empirical Bayes approach could also be used to improve estimation of the probabilities of occurrence of the additional events and conditions that would be included in any model that met the ideal requirements outlined.

5.6 Chapter summary

Several research projects have been undertaken with similar objectives to those outlined in this thesis. (Campbell and Kennedy 2003; Sotera 2007). However none fully meets the risk modelling requirements that were set out in section 3.7. These projects

nevertheless support the hypothesis that such models are desirable in the railway industry and potentially of use.

In the next chapter, Bayesian Networks (BNs) are reviewed as a potential technique with which to build models which meet the requirements for a model that have previously been outlined.

6 Bayesian Networks

In this chapter, Bayesian Networks (BNs) are introduced. I begin by describing the basic probability theory behind them, and how BNs are developed from that theory. The concepts of conditional probability, Bayes' theorem and marginalisation are then described before introducing BNs, as a technique which draws upon all of these concepts.

In the second half of this chapter, a review of how BNs have been applied to safety problems and risk analysis, in particular in the aviation industry, is presented. These reviews allow ideas to be developed for how BN models could be used to build risk models that meet the requirements for risk models that support Hypothesis 2 as set out in section 3.8. The work informs the development of the modelling approach that is outlined in subsequent chapters.

6.1 Conditional probability and Bayes Theorem

A conditional probability is the probability that one event will occur, given that another event has occurred. Where the events are a and b respectively this relationship can be written as P(a|b) (the probability of a *given* b). When events a and b are independent, P(a|b) = P(a) and P(b|a) = P(b).

Equation 3 shows the relationship between the probability of the joint event a and b, the conditional probability P(a|b) and the conditional probability P(b|a).

Equation 3: $P(a,b) = P(a \mid b)P(b) = P(b \mid a)P(a)$

The equation can be re-written as follows:

Equation 4: $P(a \mid b) = \frac{P(b \mid a)P(a)}{P(b)}$

Equation 5 is known as Bayes' Theorem, after the Reverend Thomas Bayes who first published a special case of it (Bayes 1763). Bayes' theorem is valid for all interpretations of probability. The theorem gives a formula for how to revise the strengths of evidence-based beliefs in light of new evidence. This is known as inductive – or *a posteriori* – reasoning.

Equation 4 is sometimes written as shown below:

Equation 5: $P(a \mid b,k) = \frac{P(b \mid a,k)P(a \mid k)}{P(b \mid k)}$

In Equation 5, k represents the background context on the basis of which subjective probability estimates are made, emphasising that all probabilities are conditional, and based on some background knowledge.

6.2 Use of Bayes Theorem

Taking a problem outlined by (Jenson 2001), page 7), suppose that a researcher is interested in how the sex of a person relates to the length of their hair. There are two variables of interest. Let L be the variable 'length of hair' and let S be the variable 'sex of person'.

L = {long, short}

S = {male, female}

Bayes Theorem expresses a probability which people find hard to assess in terms of probabilities that can often be drawn directly from experimental knowledge or intuition. Where conditional probability relationships exist it is often the case that one of these probabilities can more intuitively be estimated than the inverse. It is easy enough to estimate the probability that someone has long hair given knowledge of their sex. It might also be possible to estimate the probability that a person selected at random from a certain population is male. Given some background knowledge, k, a person might believe that P(male) = 0.5, P(female) = 0.5, and P(long/male) = 0.1.

'What is the probability that someone with long hair is a man?' is a more difficult question to answer. However someone would be able to calculate this from the probabilities they are able to estimate by the application of Bayes Theorem. Substitution of the estimated probabilities into Equation 5 gives:

$$P(male \mid long) = \frac{(0.1) * (0.5)}{(0.5)} = 0.12$$

6.2.1 Marginalisation

The joint event L and S represents the distribution of the two variables described above across a population. The probability of this event is written as P(L, S) and is referred to as the joint probability distribution of L and S. The probability distribution is the set of probabilities of all four possible combinations of the states of L and S: {P(long, male), P(long, female), P(short, male), P(short, female)}.

The probability of one event, without consideration of any other event is called the prior or marginal probability. If the joint probability distribution is known then the marginal

probability of any particular variable state can be calculated by the process of marginalisation (Equation 6).

Equation 6: $P(a) = \sum_i P(a, b_i)$

The value of the variable a can be determined by summing all of the products in the joint probability distribution which are calculated from a. This is because the products are mutually exclusive and exhaustive. Let us assume that we are able to estimate that:

P(long/male) = 0.1, P (long/female) = 0.7, p(short/male) = 0.9, P(short/female) = 0.3, P(male) = 0.5 and P(female) = 0.5.

Using these values Equation 3 can be applied to calculate the joint probability distribution to be:

P (L,S) = {P(long, male), P(long, female), P(short, male), P(short, female)} = {(0.05), (0.35), (0.45), (0.15)}

To calculate the probability that a given person has long hair, Equation 6 can be applied to marginalise the variable 'long' out of P(L, S):

P(long) = P(long, male) + P(long, female) = 0.05 + 0.35 = 0.40.

Therefore there is a 40% chance that a randomly selected person will have long hair.

6.3 Bayesian Networks

In this section an example introduced in ((Jenson 2001) page 7) is used to explain the concept of a BN. The example is based on the causal relationships between a person's sex (x), the length of their hair (h) and their stature (s).

6.3.1 The joint probability distribution for a number of variables

A joint probability distribution consisting of any number of variables can be calculated in this way by applying Equation 3 extended as appropriate. For example the joint probability distribution of the three variables can be calculated simply to the form:

Equation 7: $P(x, h, s) = P(x \mid h, s)P(h \mid s)P(s)$

However calculation of the full joint probability distribution becomes more complex as the number of variables and the number of states they can take increase. A BN can be used to simplify the joint probability calculation and also to provide a diagrammatic representation of the causal relationships.

6.3.2 What is a Bayesian Network?

A BN consists of a set of nodes, representing variables, and a set of directed arcs, representing influential relationships between the variables. Arcs are directed from 'parent' node to 'child' node. Each variable has a set of exhaustive, mutually exclusive states. The variables and arcs form a directed acyclic graph. The term acyclic means that there are no feedback paths through the network. Arcs model correlations between variables. The direction of the arc shows the direction of influence between two variables. The strength of the correlation is shown in the node probability table (NPT) associated with each arc.

The diagram of Figure 21 shows a BN representing the relationships between sex (x), hair length (h) and stature (s). In this example, the arcs are drawn from cause to effect creating a causal model. A probability table has been added for each node, providing the probabilities of each state of the variable. For variables without parents the table contains prior, or marginal, probabilities. Variables with parents have conditional probabilities specified for each possible combination of their parent states. The term 'BN' was coined by (Pearl 1985) because such networks substantially use subjective input information and also they rely on Bayes' theorem (as well as Equation 6), to provide the formula for calculating updated probabilities in the network.

The structure of the Bayesian Network must be developed to include all necessary conditional dependencies. A common approach is that described by ((Bedford and Cooke 2001), section 14.4) and (Smith 1989). First the relevant variables for consideration are listed. Then secondary variables, which influence the primary variables, are identified. This process is continued until it is judged that all relevant variables have been found. Each variable is then described, and assigned its possible states. The next stage is the construction of the BN. The variables are ordered $a_1,\ldots a_n$. The ordering often arises naturally for example as a result of a temporal sequence. For each i the smallest collection of variables $a_1,\ldots a_{i-1}$ is identified such that knowing these variables would make the values taken by the other variables in $a_1,\ldots a_{i-1}$ irrelevant to the prediction of a_i. The resulting set of variables is the parent set for a_1 and correspondingly a_1 is the child of each of these variables. The BN is produced by drawing a node for each variable and drawing an arc from the parent nodes identified to each of their child nodes.

A BN provides a compact representation of the joint probability distribution. In Figure 21 the states of the h and s can influence each other unless the state of x is known. h and s are said to be conditionally independent given x. The BN model therefore shows conditional independence relationships between variables. When no conditional

independences relationships are known the chain rule of probability states that the joint probability distribution of a set of variables can be calculated as follows:

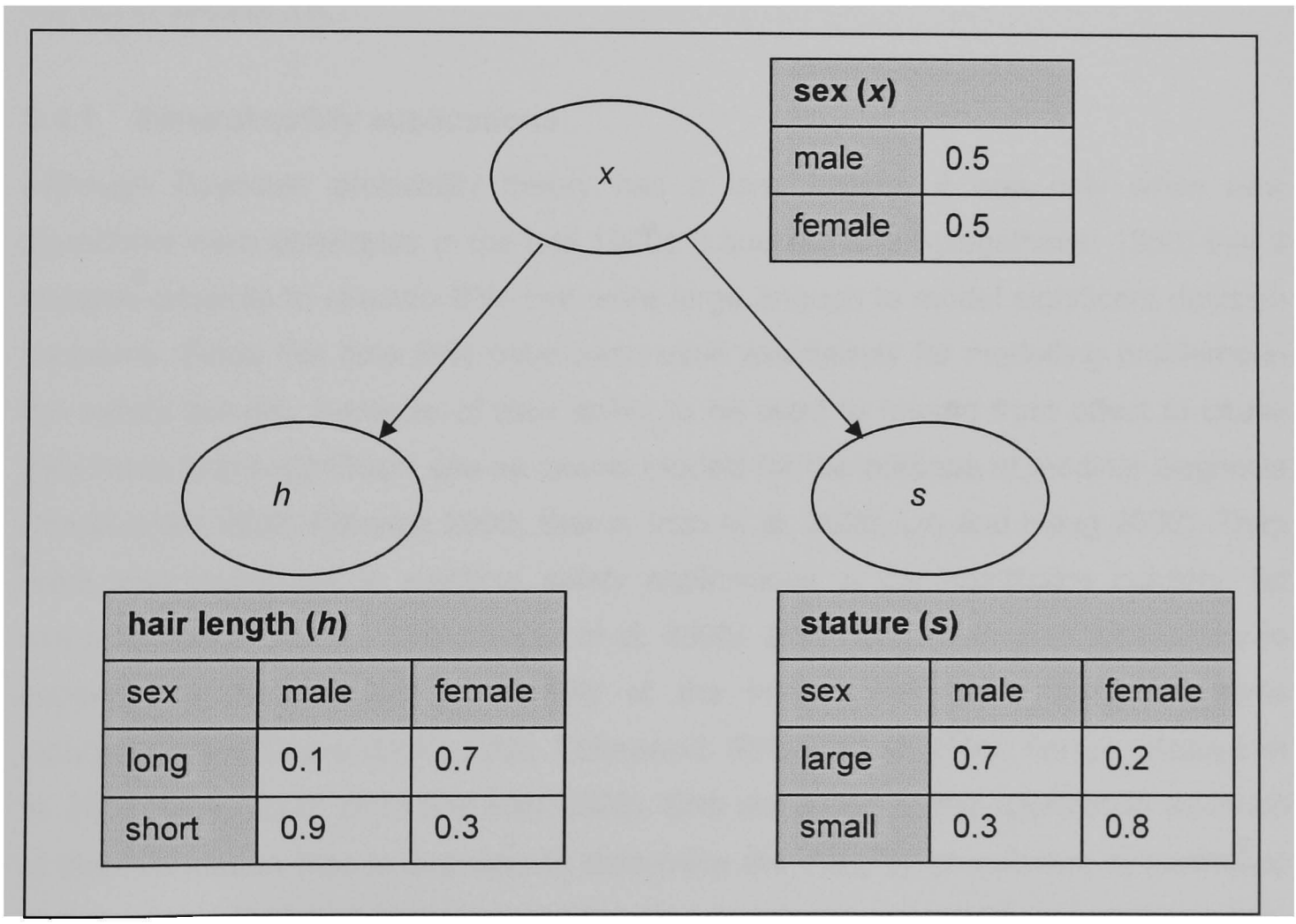
$$P(a_1, a_2 ... a_n) = \prod_i^n P(a_i \mid a_1, ..., a_{i-1})$$

The joint probability distribution is moresimple to compute when there are conditionally independent nodes and can be calculated by applying a modified form of the chain rule:

$$P(a_1, a_2 ... a_n) = \prod_i^n P(a_i \mid pa(a_i))$$

where pa(a_i) is the set of parent variables of a_i. Hence the joint distribution of the BN shown in Figure 21 is:

Equation 8: $P(x,h,s) = P(h \mid x)P(s \mid x)P(x)$ The conditional independencies expressed in the BN can be used to simplify the joint probability distribution.



sex (*x*)	
male	0.5
female	0.5

hair length (*h*)		
sex	male	female
long	0.1	0.7
short	0.9	0.3

stature (*s*)		
sex	male	female
large	0.7	0.2
small	0.3	0.8

Figure 21: BN: how a person's sex influences their stature and hair length

For larger networks the approach can result in a much simplified calculation when compared with the calculations required to apply the standard calculation of Equation

3. Software packages like AgenaRisk (Agena 2008) and Hugin (Hugin 2008) can be used to build BNs and to calculate prior and posterior probabilities from them.

6.4 Review of the use of BNs in the safety domain

In this section I review the use of BNs in safety critical and safety related applications. A detailed review of their application in three areas of particular relevance to the work described in this thesis is undertaken:

- Identification of risk hotspots
- Inclusion of operational and organizational conditions in probabilistic risk assessments
- Using BNs to extend and supplement fault and event tree analysis.

The research reviewed provides insight into how a modelling approach could be developed which produces BN models that meet or support the requirements that were set out in section 3.8.

6.4.1 General safety applications

Although Bayesian probability theory has a long history, it was only when new algorithms were developed in the late 1980s (Lauritzen and Spiegelhalter 1988) that it became possible to execute BNs that were large enough to model significant decision problems. Since this time BNs have been used extensively for modelling problems in the safety domain. Because of their ability to be used to reason from effect to cause they have found significant use as causal models for the purpose of medical diagnosis (Heckerman 1990; Nikovski 2000; Sierra, Inza et al. 2000; Lin and Haug 2008). They have also found use in systems safety applications in the healthcare industry, for example (Maglogiannis, Zafiropoulos et al. 2006). BNs have been used extensively to support the development of models of the integrity of safety critical systems incorporating software (Dahll 2000; Littlewood, Strigini et al. 2000; Fenton, Krause et al. 2001; Gran 2002; Brito and May 2006). BNs are suited to this application as much of the information that is available to determine the integrity of software is qualitative and the causal relationships that need to be considered are usually not deterministic. BNs provide a way of formalising the complicated reasoning process that is applied in such areas.

6.4.2 Identification of risk hotspots

Some research has been undertaken into the use of BNs and Bayesian statistical approaches for the identification of risk 'hotspots' across a network of installations.

6.4.2.1 Identifying hotspots on the road infrastructure

(Heydecker and Wu 2001) describe several different types of analyses that provide quantitative information about which sites across a road network would most benefit from remedial work to reduce the risk from accidents. They stress that because accidents are rare it is difficult to determine which locations have a relatively high accident frequency. Four analyses, based upon Bayesian statistical approaches, are proposed. The analyses use accident and incident data but analysis is also extended to consider a subset of the conditions that were classified in 2.3.2, namely:

- Performance conditions, for example speed limits, traffic flows.
- Technical conditions, for example road curvature.

This research shows that 'hotspot' identification is a problem for transport networks in general, not just railway networks. It also highlights that Bayesian analysis is a possible way of supplementing limited data sets to identify hotspots by incorporating belief based probability estimates rather than relying purely on data. However the approach does not draw upon or extend accepted and understood risk assessment methodologies used in the railway industry and is therefore not of direct relevance to the work described in this thesis.

6.4.2.2 PRA in the nuclear industry

Lee et al (Lee and Lee 2006) describe the application of a BN to the probabilistic risk assessment (PRA) of nuclear waste disposal. They note that PRA of a nuclear power station is possible because the power station is in a controlled and stable environment. They contrast this with nuclear waste disposal, which will occur in a variety of locations, and in which risks are dependent on environmental factors that may change significantly given the tens and hundreds of years of security that such disposals require. Lee et al are concerned with risks which are in some cases genuinely uncertain, as they may not have previously occurred at all, and therefore it is clear to see why the Bayesian approach, which is not dependent on the existence of data, is attractive to them. The approach provides a method for integrating a better understanding of variables into risk assessment. However it is tailored specifically at the problem of nuclear waste disposal, and is not suitable for use as a tool to guard against the occurrence of organizational accidents, because the modelling approach makes use of a short model of the accident event sequence.

6.4.3 Inclusion of operational and organizational conditions in probabilistic risk assessments

Several researchers have developed models which use BNs to factor organizational and other factors into probabilistic risk assessments. For example (Mosleh, Goldfeiz et al. 1997; Galan, Mosleh et al. 2007) propose a model for assessing the influence of 'organizational factors' on the reliability of components and on operator performance in probabilistic risk assessments in the nuclear industry. An 'ω factor' is developed to do this. For equipment failures the factor is calculated as the ratio of the 'inherent' failure rate to the rate of failure due to organizational conditions. An influence diagram (Mosleh, Goldfeiz et al. 1997) or BN (Galan, Mosleh et al. 2007) is used to calculate the 'ω factor' relating to operator performance by modelling the relationship between workers performance and various organizational conditions. The approach extends traditional PRA techniques and for this reason is not an approach could easily be applied to meet the modelling requirements outlined in this thesis. The objective of the research described in this thesis is to develop models which can be customised rapidly and transparently to different locations and situations without expert knowledge of PRA. Although the BN part of the model might support such an approach, the traditional aspects of the model would not for reasons already outlined: the lack of explicit modelling of conditions, and the need to replicate the model structure for similar event sequences occurring in different locations. (Oien 2001a; Oien 2001b) describes a

method of linking risk indicators to the risk assessment of an offshore petroleum installation. Again, the approach does not address the variability in risk across a range of locations that is found in the railway industry, and that the research described in this thesis seeks to address.

Other approaches are more relevant to the work described in this thesis and are reviewed in more detail in the remainder of this section.

6.4.3.1 Sensing changes in Operational Risk Exposure (SCORE)

The SCORE (Sensing Changes in Operational Risk Exposure) project (Neil, Malcolm et al. 2003; Neil 2004) was undertaken in order to determine whether it is possible to monitor changes in an organisation's safety culture, and provide a quantified assessment of the impact of such changes on risk. The work was therefore concerned with integrating operational and organizational conditions effectively into a quantitative risk model. One aspect of this work was to look at the operational risk of the air traffic control system used by the National Air Traffic Services (NATS).

The authors chose to develop the model as a BN. However, unlike the previous examples reviewed, the authors do not build the model in a single step using only expert judgement. Instead they use an existing 'barrier model' of air traffic control safety defences as their starting point:

'the conceptualisation of the processes might begin with an organogram, a pre-existing process model, or a backwards analysis of the output properties and the people and processes which contribute to those properties.'

The 'Barrier Model' (See Figure 31) consists of various events in the aircraft collision accident sequence (potential conflict, projected conflicts, loss of separation and accident). These events are separated by procedural barriers, which are intended to prevent the occurrence of each successive event in the sequence.

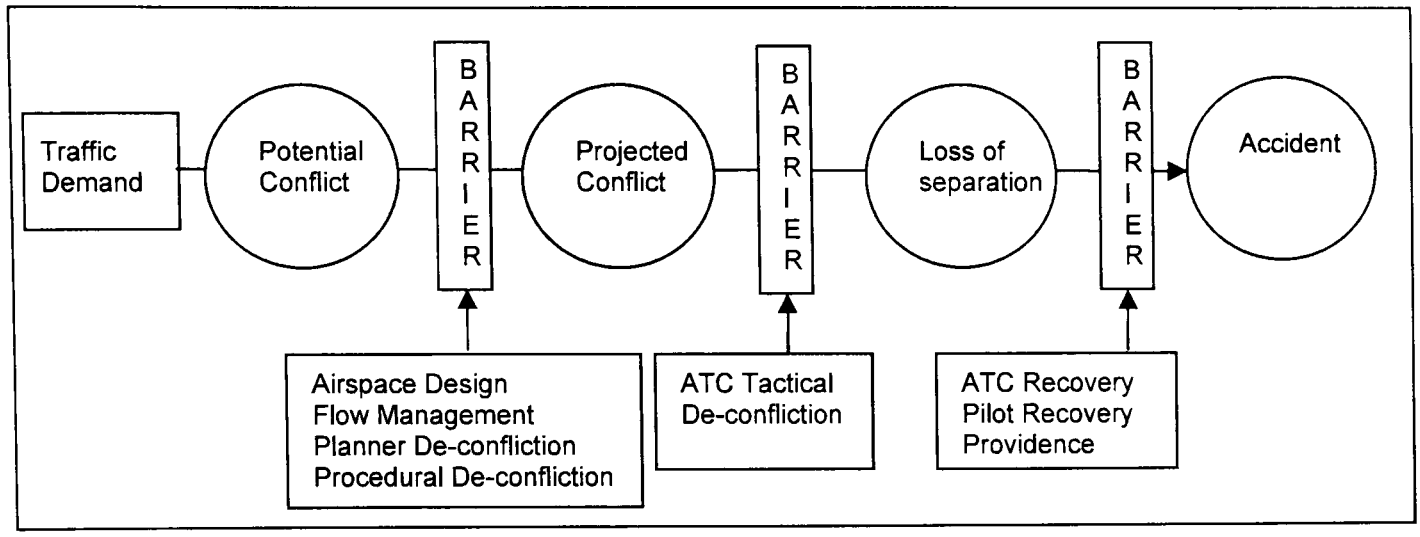


Figure 22: Air Traffic Control 'barrier model'

The use of a barrier model, which is essentially a representation of the 'defences in depth' that are in place to prevent mid-air collision of aircraft, indicates that this research, like the research described in this thesis, is concerned with the development of models to prevent the occurrence of organizational accidents. The use of the 'barrier model' as a conceptual model to inform the building of the BN is sensible for a number of reasons. The model used is understood by the experts within NATS whose advice was sought when building the BN. These same people are those that ultimately would be best placed to use the BN model. The barrier model provides simple alternative representation of the problem that can be used for explanation to the lay person if necessary.

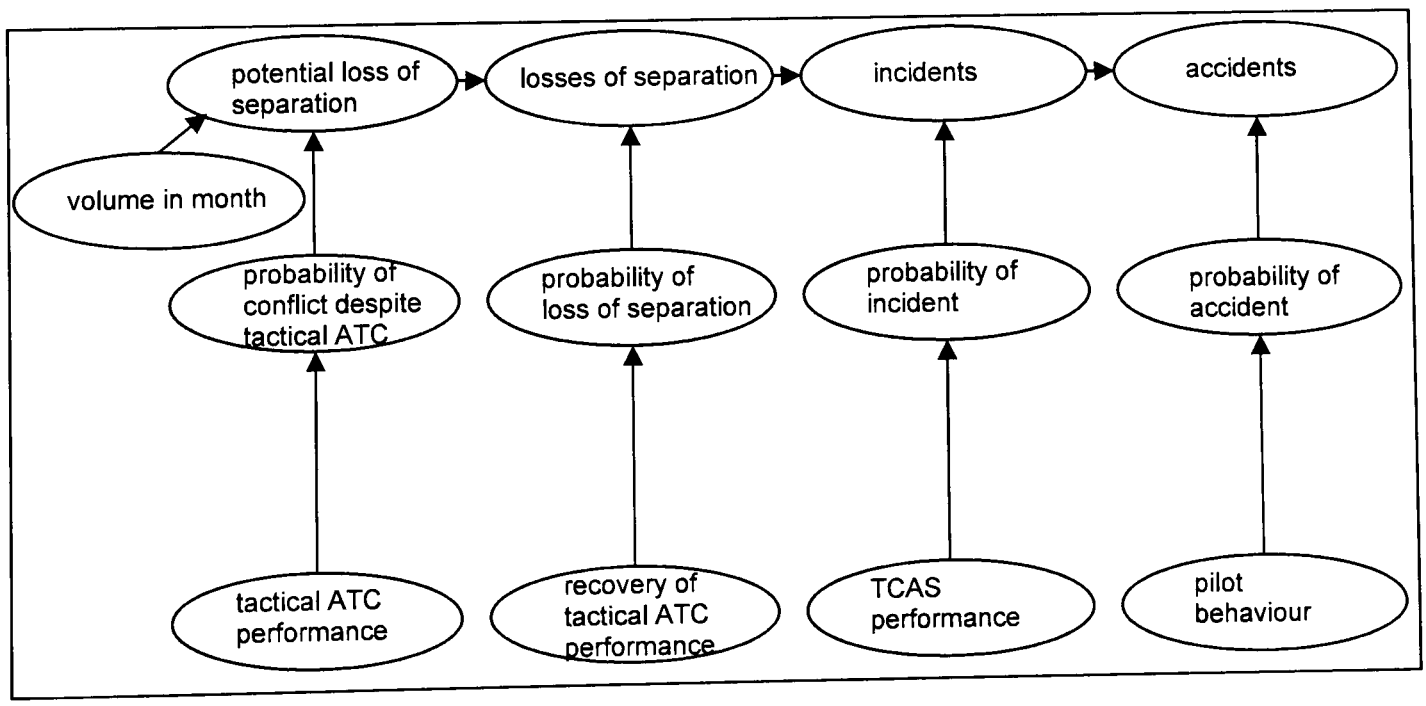


Figure 23: BN representation of the air traffic control 'barrier model'

Figure 23 shows the subset of nodes in the resulting BN that represent the barrier model shown in Figure 22. The BN is not an exact translation of the barrier model. For example, a distinction has been made in the BN between incidents and accidents in the

event sequence to take into account the potential for the Traffic Collision Avoidance System (TCAS) to prevent the occurrence of an accident.

The performance of the barriers is modelled in the nodes at the bottom of the diagram. For example 'tactical ATC performance' might be 'good' or it might be 'poor'. These categories were assigned on the basis of expert judgement of ATC performance based on judgements about levels of performance relative to a perceived normal performance. To support this process questionnaires were completed and audits undertaken of a number of different ATC teams. The level of performance influences the effectiveness of the barrier at preventing an event from escalating to a subsequent more serious event. Hence 'probability of conflict despite tactical ATC' takes on values representing the probability of occurrence of a breach of the barrier, per demand on the barrier, given the performance of tactical air traffic control. The demand on each barrier is modelled using the chain of nodes at the top of the diagram. The node 'volume in month' models the volume of traffic that is handled in a month and hence the number of demands on the first barrier. Depending on the probability of each of the procedural barriers failing to contain an event, proportions of this traffic are calculated as breaching some or all of the procedural barriers.

There are many more nodes in the full net besides these nodes shown in Figure 23. Other nodes are used to model 'socio-technical functions'. Figure 24 shows the BN nodes modelling the socio-technical function for tactical air traffic control.

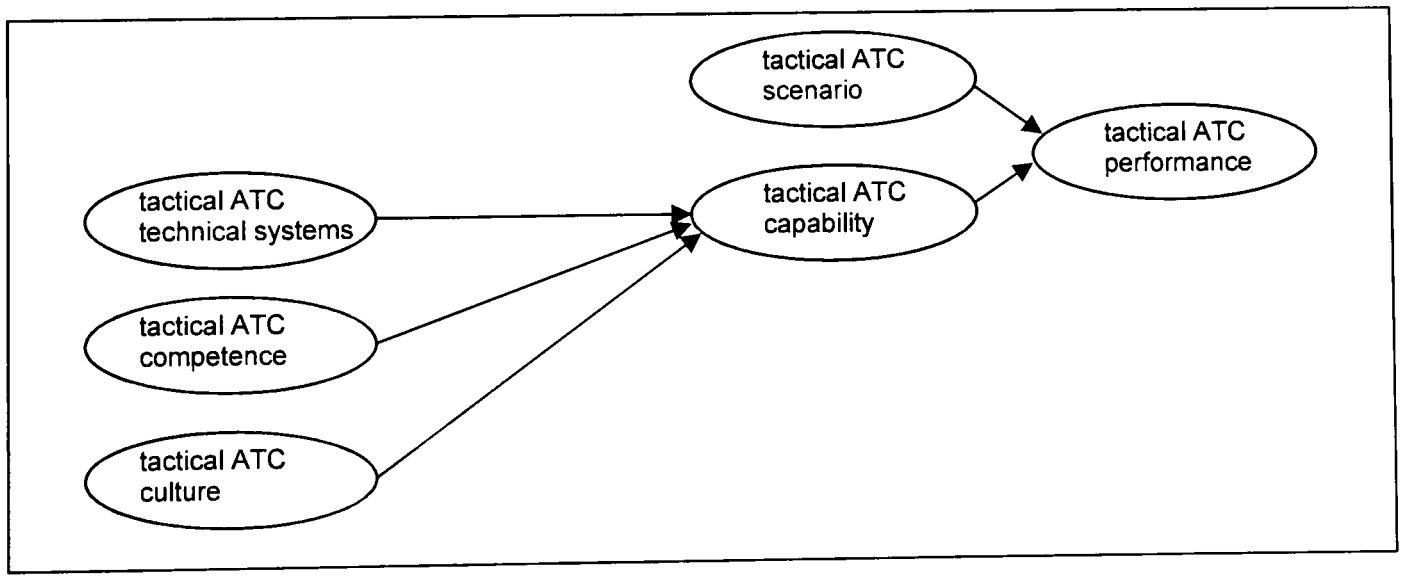


Figure 24: Air traffic control BN fragment

There are various influences that affect the performance of socio-technical functions. Process models are used to break down the causal relationships between these influences and the performance node in a structured way. The authors make use of BN idioms (Neil, Fenton et al. 2000). BN idioms are sets of linked BN nodes that represent tried and trusted models of causal mechanisms. Ultimately the BN provides causal

links between measurable quantities, like safety culture indicators and audit results, and the likelihood of occurrence of events in the accident sequence.

The authors acknowledge difficulty in building such models in particular in ensuring clarity and consistency in what the nodes actually represent. They point out that the meaning of nodes can shift subtly as the BN is edited and that a clear understanding of the entities involved (e.g. people or teams) and the particular tasks they are undertaking is essential.

There are two key aspects of the work that highlight the way forward for the work described in this thesis. The first is the use of a conceptual model as the starting point for the development of a BN. BNs are attractive for complicated modelling problems because of their inherent flexibility and adaptability. However, if an unstructured approach is followed this flexibility can result in the building of an over-complicated and confused model. The structure of the model needs to be constrained in some way and the use of a conceptual model, in this case the barrier model, is a potential way to do this. A conceptual model also aids in the ability of others to understand what the model represents, whether they are developing it or using it. Yet the translation between the barrier model and the BN in this example is only an informal one. There are no clear rules to define the translation of one model to another. If it were possible to use a conceptual model to define the structure of a BN more formally then one could use the model as a specification for part of the net. This might aid in the validation of the final model, as well as helping in the understanding and interpretation of the model. The SCORE researchers acknowledge the difficulty of validating BN models.

The barrier model is suitable for use as a conceptual model for the aviation problem addressed by SCORE. It can be assumed, with justification, that there is a single consequence of mid-air collision: a major accident resulting in the loss of two planes and the lives of all aboard them. The event sequence leading to the accident is also fairly well defined. The event sequence can therefore be fairly well represented using the linear causal structure of the barrier model.

To adopt this approach for the railway industry a different, less simplistic, conceptual model is needed. In the railway a wide range of contributory causes of an accident are often relevant with a range of different potential outcomes, the severity of which will be variable. Therefore a more complicated, branching structure of events is required. The conceptual models in wide use in the railway industry are fault and event trees and these would seem to be sensible models on which to base BN models for the railway industry. There is also much more numerical and logical information encoded into fault

and event trees than there is in barrier models. This information could potentially be adopted to help quantify the BN. If fault trees and event trees could be used as conceptual models, and the translations between them made more formal, then this additional information would also help the model building and validation process. Various entities and functions are relevant when determining what the influences on particular events are.

The second key aspect of the work that indicates a way forward for the work described in this thesis is the ability to model conditions. The work shows that conditions can be effectively modelled in BNs. In the diagram of Figure 24 the capability of the ATC team is influenced by 'culture' and 'competence' of the team, conditions whose state affects the likelihood of occurrence of an accident. BNs provide a means to develop a model which includes the technical, operational and organizational conditions that were previously identified as key to the occurrence of accidents.

6.4.3.2 An aviation BN causal model

In two supporting papers, Roelen et al (Roelen, Wever et al. 2003a; Roelen, Wever et al. 2003b) outline an approach for using BNs to model the technical and managerial causes of aviation accidents at airports that has progressed concurrently with the work described in this thesis. Their paper describes two cases studies. One considers the causes of 'missed approach' incidents, where planes should abort on approach to landing because of undesirable landing conditions. The other considers the causes of flight crew fatigue, which itself is a potential cause of a number of aviation accidents. The authors argue that improvements in causal modelling are needed in the aviation industry for much the same reasons as those highlighted in section 1.4. Aviation systems (like systems in the railway industry) have a high degree of technical and procedural protection and are largely proof against single failures, making them prone to 'organizational accidents'. To capture this phenomenon models need to include procedural and managerial failures. They argue that this is not possible using a tree type structure as the tree would need to be very complex and would become unmanageable. Instead they only develop their tree to a level where common mode influences manifest themselves. They also argue that fault and event trees are poor for modelling human factors and organizational behaviour and in particular they stress the binary nature of fault trees, and the inability to model sequence dependencies within them. They propose the use of BNs to develop the causal model because this technique is inherently flexible, and can be used to model widely differing types of causal relationships. A distinction is made in their BN between the 'technical model'

and the 'management model'. The paper does not make the reasons for this distinction clear, but the technical model is considered to be a model of 'the accident risk', whereas the management model captures the processes that are carried out within the aviation system. Both models are considered to be 'holistic' in nature rather than 'deterministic' a property that the authors believe is exhibited by classic QRA techniques like fault and event trees. This distinction appears to be based on the clarity and strength of the causal relationships between variables. In fault and event trees 'events', rather than 'influences', are modelled. Each event usually has only two states ('occur' and 'not occur') and often the occurrence of one event definitively determines the occurrence of another. The causal relationships modelled here, and captured in the BN, are less well defined. They depend on the particular state of a number of multi-state variables and weak causal relationships often exist.

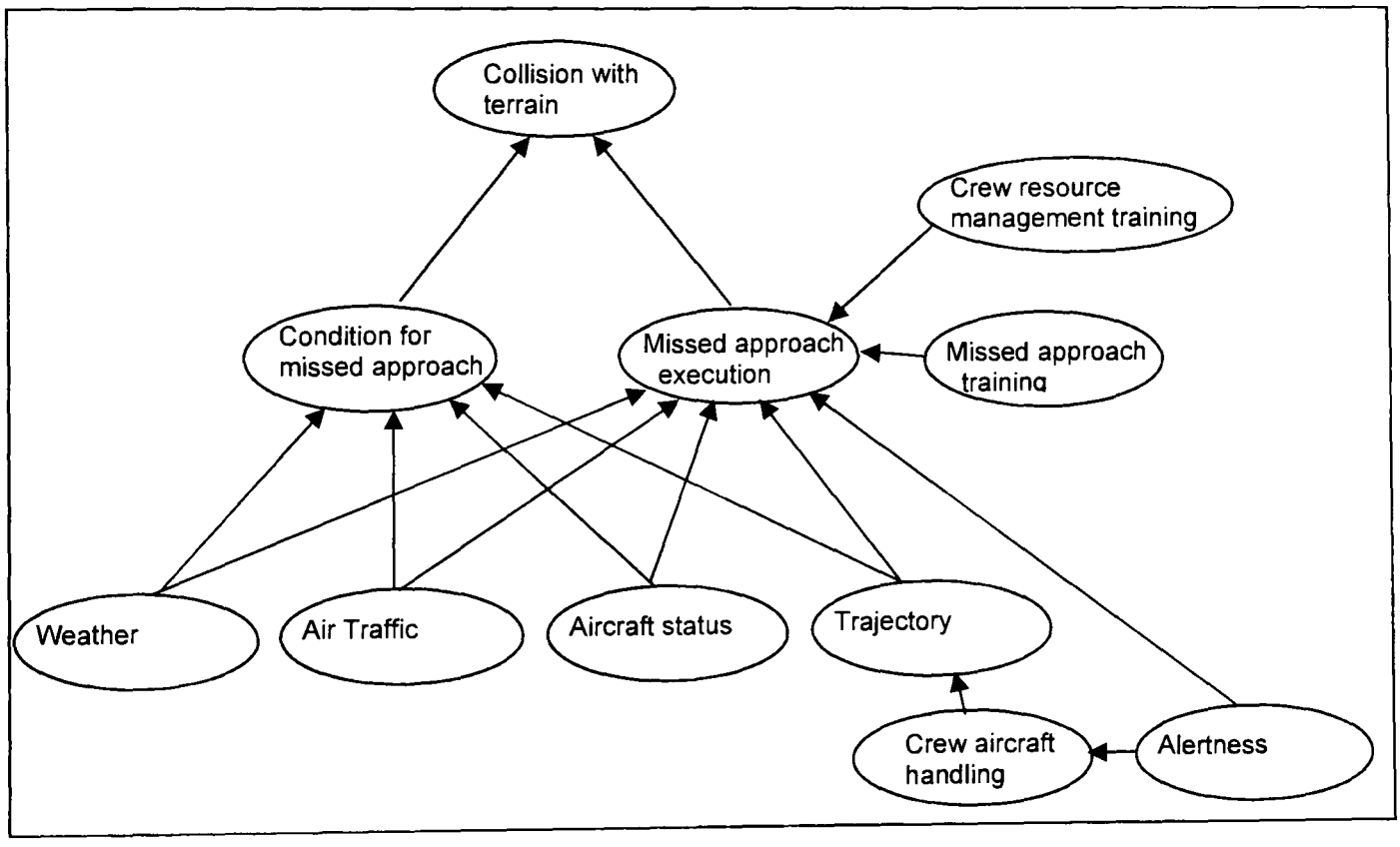


Figure 25 BN modelling missed approach of a plane to an airport runway

Figure 25 (Roelen, Wever et al. 2003b) shows the BN causal model for missed approach. The variables comprising the technical model are shown using transparent BN nodes. The authors acknowledge that assessments must be well documented to avoid them becoming slipshod and non-traceable but they do not provide any guidance as to how this should be done.

As with the SCORE research, this project highlights the ability of BNs to be used to model conditions as causal factors. Conditions do not definitely cause an accident, but increase its probability of occurrence, and BNs can be used to represent such relationships. However the model chooses to discard the fault and event tree

representation. The authors highlight the difficulty of using fault trees for detailed causal analysis that were highlighted in Chapter 4 when reviewing the structure of the SRM, and the Risk Solutions derailment model.

'[Modelling causes at a detailed level of abstraction] leads to a combinatorial explosion of the tree, which cannot be handled quantitatively' ((Roelen, Wever et al. 2003b) p 1322)

By abandoning the fault and event tree structure and the constraints that it places on the model, some rigour in the model development process has been lost. The model makes no conceptual distinction between events (such as missed approach execution) and conditions (such as weather conditions or alertness). Only the former are capable of being explicitly modelled in fault and event trees. There are arguably only two events in the BN model 'Missed approach execution' and 'Collision with terrain'. Ideally the complete sequence of events leading to an accident, and all of the diffuse conditions that affect the probabilities of occurrence of these events would be modelled. The truncated sequence of events presents a scope limitation of the model.

In building the model in this way the authors have also discarded many of the concepts that safety engineers apply, and find useful when deciding how to manage safety. In other words, the model does not represent the causal structure of events in the way that a safety engineer would expect to see them. There is no hazard identified and the accident is not clearly distinguished.

One key finding of this work is the possibility of using BNs to model correlations between seemingly independent events and conditions in the model. This is potentially very valuable.

A similar project has been undertaken to produce causal models to help understand how the risk from low probability, high consequence accidents changes when new technology is introduced into a system (Roelen, Wever et al. 2003a). Again the BN developed makes no use of the fault and event tree structure, or standard safety engineering concepts. The BN model built includes only variables such as 'organizational climate' and 'training' which are more difficult to define than events, and which are linked with weak influential causal relationships.

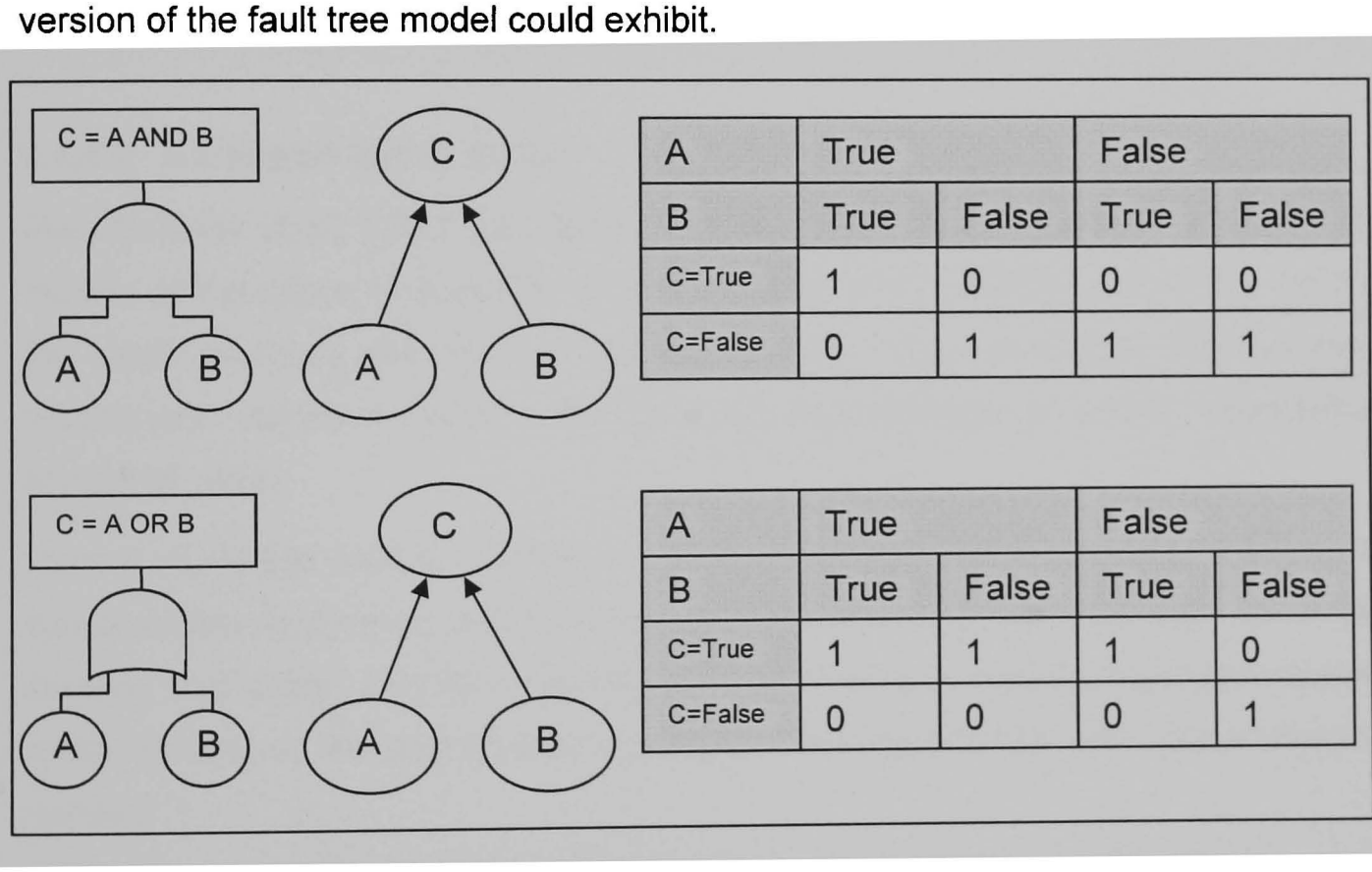
6.4.4 Using BNs to extend and supplement the accepted modelling techniques.

Several research projects have been undertaken which seek to use BNs to extend the use of the accepted method for undertaking risk assessment, fault and event tree

analysis. As such approaches build on approaches which are accepted within the UK railway industry they are of particular relevance to the work described in this thesis.

6.4.4.1 Translating Fault Trees into BN format

Bobbio et al (Bobbio, Portinale et al. 2001) outline how any fault tree can be directly translated into an equivalent BN. This translation is investigated to consider the uses of BNs within the fields of reliability and dependability analysis, for which fault trees were originally developed. Figure 26 shows fault tree AND and OR gates and their BN equivalents. The conditional probability tables for the nodes representing the gate output variables are also shown. The BN produced, like the fault tree, can be used to calculate the top event probability, given the probabilities of occurrence of base events. However, the authors' interest is in the additional functionality that the resulting BN version of the fault tree model could exhibit.



A	True		False	
B	True	False	True	False
C=True	1	0	0	0
C=False	0	1	1	1

A	True		False	
B	True	False	True	False
C=True	1	1	1	0
C=False	0	0	0	1

Figure 26: BN equivalents of fault tree AND and OR gates

The basic underlying assumptions, and therefore constraints, of the fault tree methodology are listed, such as:

- events are binary events (working/not working);
- events are statistically independent
- relationships between events and causes are represented by logical AND and OR gates

The paper shows how by converting a fault tree into its equivalent BN, these assumptions can be 'relaxed' in the resulting model and therefore it can be applied

more flexibly to reliability modelling problems. For example, the authors describe how the BN can be adapted to model multi-state variables. Using an example from digital electronics, they illustrate how a base event could be modelled that had three states: 'working correctly', 'stuck at 0 fault', and 'stuck at 1 fault'. They also describe how common cause factors can be easily modelled in the BN NPTs. The ability to introduce uncertainty into the deterministic logical rules (e.g. AND and OR gates) is also discussed *'[logic] gates may reflect an imperfect knowledge of the system behaviour....'* ((Bobbio, Portinale et al. 2001), page 254).

This research illustrates the ease with which fault trees can be translated into BNs, and that fixed rules for how to do this can be described. The increased flexibility of use demonstrated by Bobbio et al could be used to improve the capability of such models to represent technical, operational and organizational conditions, although the authors do not acknowledge or investigate this.

6.4.4.2 An airport safety model

(Ale, Bellamy et al. 2006; Ale, Bellamy et al. 2007) have used BNs to build hybrid models of the cause of accidents at airports. The high level objectives of the work are the same as those described in this thesis. They argue that more detailed causal models are needed to capture the particular circumstances in which 'organizational accidents' occur.

'causal modelling enables policies and inspection regimes to be tailor made to the vulnerabilities in systems and to those activities that pose the most risk...for a more detailed and airport specific assessment of the risks a correspondingly more detailed understanding of the pathways to accidents, their probabilities and consequences is needed'

The approach they describe has evolved concurrently with the work described in this thesis. In (Ale, Bellamy et al. 2006) they describe a programme of work to develop causal models in the aviation industry. In their most recent paper (Ale, Bellamy et al. 2007) Ale at al propose the use of event sequence diagrams, BNs and fault trees together to model accident causation in and around Schipol airport. Ale et al use fault trees as part of the underlying BN specification, as proposed by Bobbio. The approach proposed has many similarities to the work that will be described in Chapters 7 and 8. In particular a single integrated BN, developed from alternative causal models, is used to undertake calculation. They see this as a way to ensure *'consistent handling of probabilities and their interdependence'* ((Ale, Bellamy et al. 2007), page 1438).

The model they describe focuses on variations in situation. This contrasts with the primary focus of the model proposed in this thesis on variability associated with location. The BN therefore primarily extends their model to include variability in operational conditions on the basis that human performance is the potential source of most variability in accident likelihood that might be expected at any given airport.

6.4.4.3 A maritime model

(Trucco, Cagno et al. 2007) describe a case study in the maritime transportation sector which uses Bayeisan Networks to integrate 'human and organizational factors' into a probabilistic risk analysis. A BN is developed of the operational and organizational conditions. Correlations are then identified between the model and the base events of a fault trees that had previously been developed to estimate the risk from collision accidents in the open sea. To develop the BN part of the model the authors translate functions from another approach, the Structured Analysis and Design Technique (SADT) into a BN formalism.

The authors argue that the model can be used to identify opportunities for risk mitigation acting at an organizational or regulatory level. They also argue that it could be used to support retrospective analysis, such as the identification of latent organizational failures using accident and incident data.

The approach illustrates the potential for BNs and fault trees to be merged into a similar model. However it only considers the causal side of the accident sequence. Also, it only makes operational and organizational conditions that underpin the fault tree base events explicit as underlying assumptions. The objective of the work described in this thesis is to develop models that make all assumptions, including performance and technical conditions, both explicit and variable. The omission of such causal factors limits the ability of the approach to be used in a range of circumstances and locations.

6.5 Improving risk models using BNs

The literature review undertaken provides evidence that BNs provide a technique with which it may be possible to build a risk model which meets the ideal requirements previously set out.

Our first requirement for a model (RMR1) is that risk models should allow as many of the events in an accident sequence to be modelled as is practicable. Earlier reviews demonstrated the possible accident event sequences could be modelled in fault and

event trees. The work described in this chapter shows that BN versions of fault trees can be developed using BNs. Bobbio describes how to translate fault tree models into BNs using clear and repeatable rules (see section 6.4.4.1). A similar translation from event trees to BNs would be needed in order to develop a BN version of the standard accident event models used in the industry (this is investigated in the next chapter). .

The second requirement is that 'Risk models should allow all significant and quantifiable technical, operational, organizational and performance causes of accidents to be explicitly modelled.' The research reviewed shows that BNs have previously been used to make certain types of conditions explicit and variable in a BN. Previous research therefore gives confidence that once an underlying BN event model has been produced it could be extended, by adding nodes that represent all conditions of interest.

A range of projects have been undertaken that use BNs to incorporate operational and organizational conditions into risk models (see section 6.4.3). These conditions are of a transient nature and making them explicit in the model as BN nodes allows the impact of their change to be modelled and its effect on risk to be calculated. The BN also provides a qualitative model of the causal relationships between organizational and operational conditions and risk.

Requirement RMR3 is that 'Risk models should be parameterised by conditions so that the risk at different locations and in different situations on the railway network can be rapidly recalculated.' BNs provide a candidate technique to use to develop a risk modelling approach with this capability. There is evidence that it is possible to identify and model the occurrence of risk hotspots using Bayesian approaches (see section 6.4.2) All relevant work found uses Bayesian statistical approaches to allow belief based estimates to be used to supplement location specific data which tends to be incomplete. Conditions may be correlated to each other, or they may introduce correlations between events. As was discussed in section 2.4.4, when conditions affect both the fault and event tree this has the potential to introduce inconsistencies between the fault and event tree parts of a risk model. BNs can be used to model correlations between any nodes in a model. Therefore, if a model included all events and conditions of interest, the correlations between them could be explicitly modelled. This would ensure that their impact was appropriately considered when the model was customised to model the risk at a particular location

Another of the requirements (SDM1) is that 'In order to ensure that they effectively support the taking of safety related decisions, risk models should be usable and understandable by those who actually manage safety on the network.'

In order to develop a complex BN model, it is sensible to start with an existing model. Both the SCORE work (Neil, Malcolm et al. 2003; Neil 2004) - see section 6.4.3.1 - and the research undertaken by (Ale, Bellamy et al. 2006; Ale, Bellamy et al. 2007) – see section 6.4.4.2 - develop BNs from existing, risk models produced using accepted and understood approaches. Neil, Malcolm et al use a barrier model, whereas Ale, Bellamy et al use fault trees and event sequence diagrams. This approach helps to structure the BN and also provides an alternative causal model which can aid interpretation of the results of a BN, and can help in its validation. To build a BN, one should start with an underlying conceptual model. The risk modelling approach envisaged would begin with a model of the accident event sequence at its 'spine'. This part of the model can be effectively captured using fault and event trees. Fault and event tree models are not just the computational models that safety engineers use in the railway industry. They also represent the conceptual model that engineers use to reason about safety and risk. It is clear that these models would therefore provide the sensible underlying conceptual model for a BN model of risk in the railway industry.

6.6 Chapter summary

In this chapter I described BNs (BNs) and the underlying theory that supports them. I then investigated how BN models have previously been used in the safety domain and in particular for probabilistic risk assessment. This review of the research allowed some clarification of ideas for how it might be possible to develop a modelling approach that meets the ideal requirements set out in section 3.8. The key clarifications are that:

- BNs provide a potential technology on which to base a modelling approach.
- The methodology should be based on the use of fault and event tree models as an underlying specification for the BN.
- A modelling approach based on the use of BNs has the potential to meet the requirements for an ideal UK railway risk model that were set out in section 3.7.

Previous research has established how to develop BNs from fault trees. In the next chapter I investigate how to undertake a translation from event trees to BNs. This process is the formalised, as a step towards the development of an ideal UK railway risk modelling approach.

In the next two chapters, a case study is described which illustrates a new approach to modelling risk in the UK railway industry based on the development of a parameterised risk model using a BN.

7 Case Study Part 1: Parameterising event trees using Bayesian Networks

In the next two chapters, a case study is described which illustrates a new approach to modelling risk in the UK railway industry, based on the development of a parameterised risk model using a BN. The case study develops, and is based on, the industry risk analysis that were introduced in section 4.3.1.

These chapters provide the argument in support of Hypothesis 3 (that the development of a risk modelling approach with characteristics suited to use in the UK railway industry is possible).

In this chapter, the first part of the case study is outlined: the development of a parameterised BN based on the structure of the set of event trees from the industry derailment analysis. The case study describes how the event trees can be used to develop a BN model which incorporates all event tree logic and also makes the condition states that form the underlying assumptions of the initial analysis both explicit and variable.

First, in section 7.1, the production of a BN equivalent of an event tree is described. Then, in section 7.2, the industry risk analysis introduced in section 4.3.1 is revisited to show how an event tree modelling the risk from train derailment at a particular location can be translated into a BN by following this approach. Section 7.3 demonstrates how to include conditions, whose states form the underlying assumptions of the event tree, as BN nodes. The relationships between the states of those conditions and event probabilities are elicited, and a more general model produced as a result. This process is referred to as parameterisation of the model.

In section 7.4, a large event tree that includes all of the derailment event sequences that exist from the full set of event trees developed for the industry analysis is described. This model is again translated to its BN equivalent and parameterised by the addition of condition nodes and elicitation of causal relationships. The original study consists of a number of different event trees, each representing different locations, where particular combinations of condition states are assumed to exist. When the condition states that were assumed for each of the initial analyses are selected in the resulting BN and the evidence propagated through the net, the model calculates the same output as each initial event tree. However, using the model it is also possible to analyse the effect of entirely new combinations of condition states on accident probability.

For each parameterised BN model shown the output of the model is investigated to gauge whether the approach produces models that give sensible results and to provide insight into how these types of models might be able to be used in the railway industry.

7.1 Simple translation from an event tree to a BN

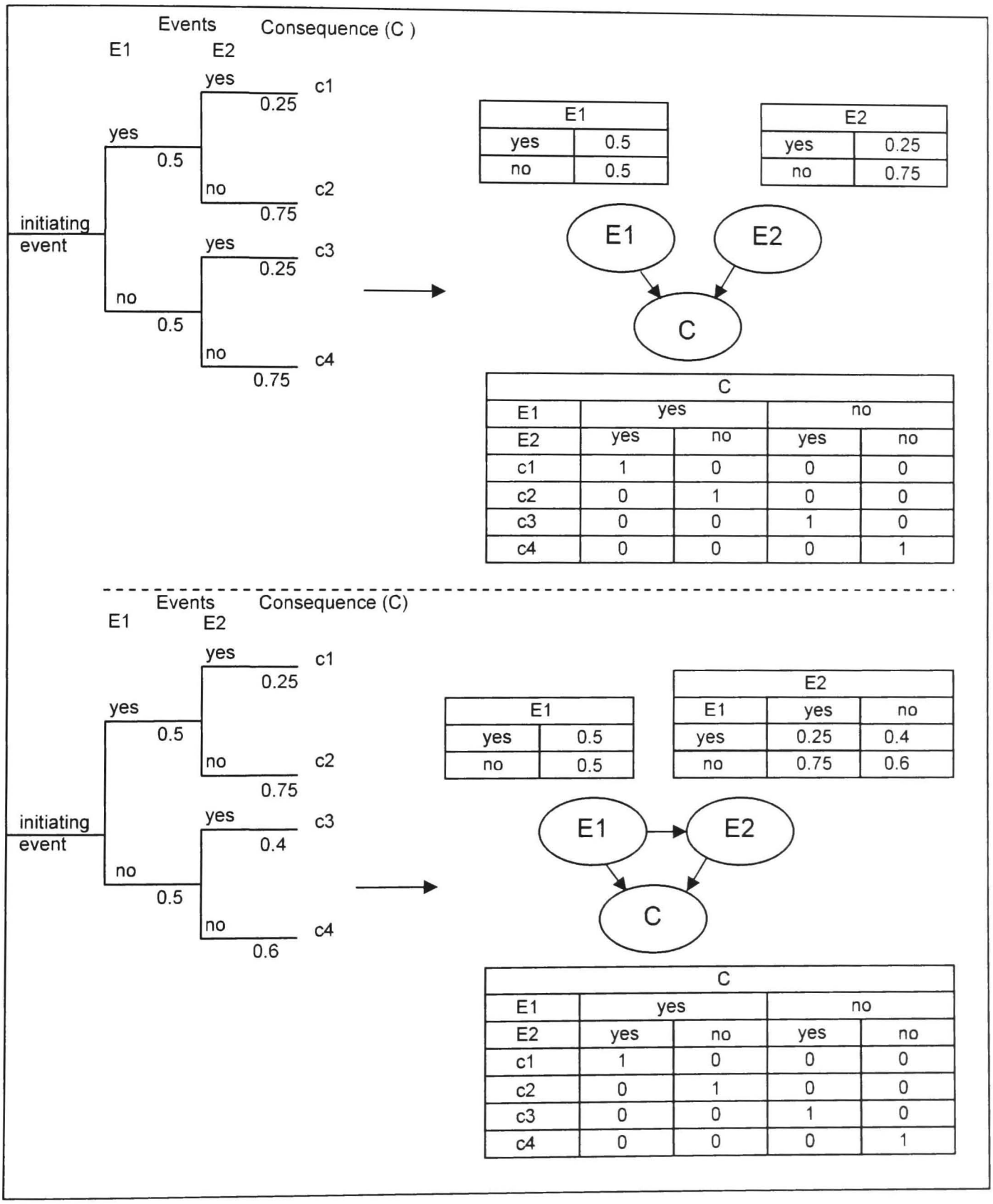


Figure 27: Fundamental principles for the translation of event trees into BNs

Figure 27 shows two fully expanded event trees and their BN equivalents. Each event tree has two events. The translation to BNs is substantially the same for both event trees. In both cases, BN nodes E1 and E2 are needed for each event in the tree. Event

nodes have a state for each of their possible outcomes (yes and no). The probabilities of occurrence of each event are taken directly from the event tree. BN node C is also needed in both cases to represent consequences and this node has a state for each possible consequence (c1-c4). The derailment consequence is determined by the combination of events that have occurred. Therefore arcs are needed from each event node to the consequence node.

The key difference in the rules for translating the two event trees in Figure 27 is that in the first there is no conditional probability relationship between events but in the second there is. This information is implicitly shown in the event tree. In the bottom event tree we see that the probability of occurrence of E2 differs depending on whether or not event E1 has occurred. However, in the top event tree the probabilities of occurrence of E2 is unchanged. This shows that in the bottom event tree E2 is conditionally dependent upon the outcome of E1 and an additional arc is needed in the BN to represent this. The diagram shows how all NPTs would be quantified in the resulting BNs. Conditional dependencies do not have to be between consecutive events in the event tree. Where larger event trees are built, which consist of a greater number of events, an event could be conditioned upon the outcome of one or more of its preceding events.

(Kastenberg, Apostolakis et al. 1993) describe a translation between decision trees and influence diagrams. Their approach is similar to the one described here, given the similarity of those modelling techniques with event trees and Bayesian Networks respectively.

7.2 The core derailment study revisited

For the purposes of the case study, the 'derailment study' that was reviewed in 4.3.1 is now revisited. In that study, six separate derailment risk models were built, one for each of the different types of location that were together considered to be representative of the infrastructure being analysed. These models were:

- derailment on open track, where the train is not adjacent to any significant infrastructure or enclosed by a tunnel
- derailment in a station, when stopping at that station
- derailment inside a tunnel
- derailment on approach to a tunnel
- derailment when passing through a station (not stopping)

- derailment on bridges or viaducts

As was discussed in section 4.3.2 this approach introduces an inherent simplification. The approach assumes that there are only six possible and distinct sets of conditions arising on the section of the network analysed.

The severity of each possible outcome indicated in the event tree was calculated externally to the model using a range of variables, such as train speed, the type of rolling stock, passenger loading, and the particular consequence indicated, for example whether or not any secondary collisions occurred.

7.3 Parameterisation of a single event tree

In this section, a single event tree from the derailment study is used to demonstrate how the approach described in Figure 27 would be applied in practice. Then the 'parameterisation' of the resulting BN version of this event tree is described. This process involves making the conditions that form the underlying assumptions of the event tree explicit in the model, and eliciting the causal relationships between event and condition nodes.

7.3.1 Translation of an event tree into a BN

The event tree produced to model derailment consequences in areas of 'Open Track' is shown in Figure 28. The event tree shows the probabilities of occurrence of each of 12 potential consequences, given that an initial derailment has occurred. The model is underpinned by a number of assumptions that relate to the core derailment study. These assumptions were clarified and summarised previously (Table 5) and the meaning of each event at the top of the event tree was also previously described (Table 4).

The event tree shows a range of probabilities associated with each event tree branch and the various outcome probabilities that were calculated using this tree. The event 'contained' is redundant as the assumption is made that no containment rail is fitted anywhere on the section of infrastructure modelled for the core derailment study. The event 'contained' is included in the model because the event tree branching structure is taken directly from the derailment study previously reviewed which included it.

The SRM is based on a much wider geographical scope, and includes some areas of infrastructure where containment rails are fitted. Rather than edit the tree to remove its uppermost branch this structure is retained as it impacts upon the BN structure that is subsequently built.

In order to translate the event tree into a BN, the same approach as is described on section 7.1 is applied. One node is created for each of the events in the event tree. A single consequence node that is influenced by all possible events is then added. The consequence node has 12 possible states, one for each possible derailment consequence. For the purposes of this case study it was considered sensible to use the events from the SRM derailment event trees as probabilities associated with the occurrence of these events, given certain assumed condition states, were readily available. The existing models show that quantification of probabilities of occurrence for these events is credible. This results in a model of similar complexity to an industry standard model, with similar potential uses, whilst minimising the need for additional data analysis and expert judgement. Figure 28 shows that there are two separate branches of the event tree where it is possible that a derailed train will hit a lineside structure. The probability of a derailed train hitting a lineside structure is different in each case. This shows that the probability is conditionally dependent on whether or not the train has fallen over.

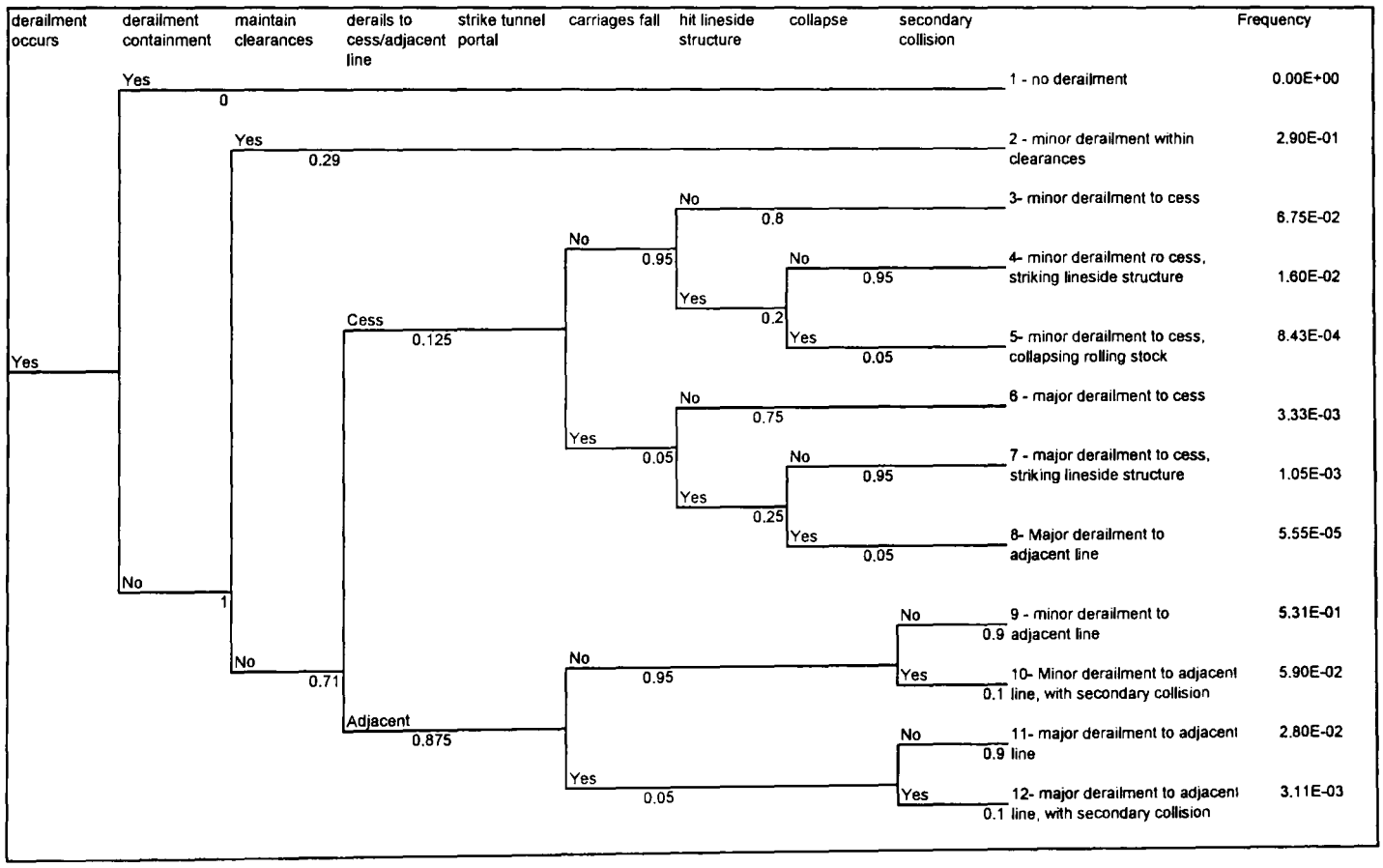


Figure 28: Open track on a busy commuter railway

An additional arc is added between the node 'falls' and the node 'hits structure' to model the conditional probability relationship that is implicit in the event tree. The difference in probabilities is small, representing a weak correlation between the events. The analyst's judgement that this correlation is weak was based on the view that, following a derailment, a train will be likely to travel a greater distance if it remains upright, and hence is more likely to collide with a structure at the side of the track. Note

that this is the only place in the event tree where event probabilities differ according to the events that have preceded their occurrence. The BN produced is shown in Figure 29.

Comparing the 'open track' derailment event tree with its BN equivalent shows:

- The logical combination of events leading to each accident is most clearly shown in the event tree.
- The occurrence of conditional probabilities – arising from dependence between the events – is shown more clearly in the BN.

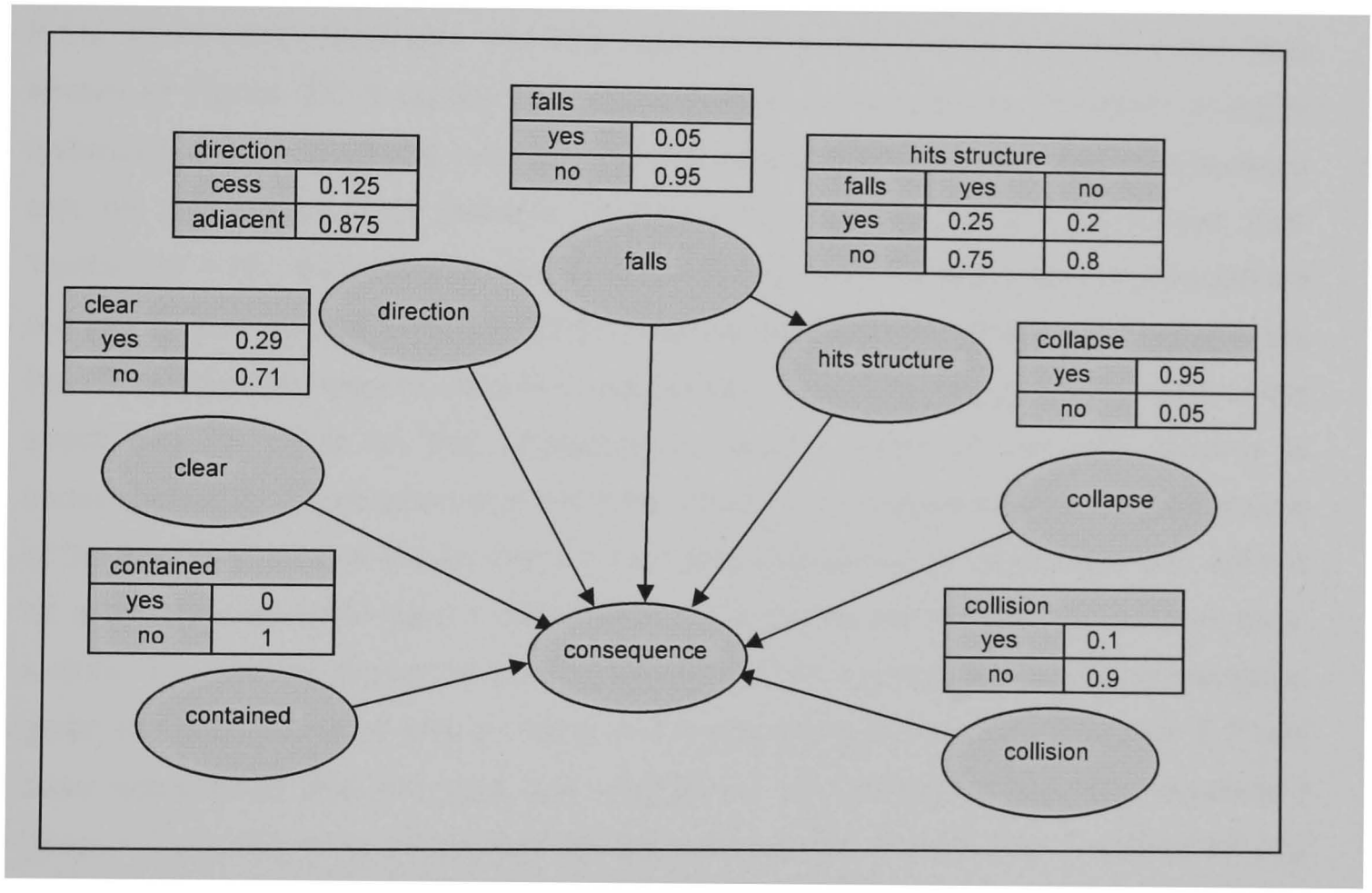


Figure 29: BN event tree for derailments on a section of open track

The models provide complementary representations of the event sequences. The fully expanded event tree model would have 2^7 (128) different consequence endpoints. These need to be mapped to the 12 different modelled consequences in the 'consequence' node. Therefore, using the BN structure shown, the 'consequence' NPT would contain 1536 different entries, one for each of the 12 consequences under all 128 different condition combinations. To simplify the quantification of the 'consequence' a different BN structure is used in practice (the structure is shown in full in Appendix B1.1). The consequence node is broken down into a number of sub-nodes. Each sub-node models a subset of the consequence states and is dependent on the minimum

subset of events on which these consequence states depend. With reference to Figure 28, for example, if we know that 'carriages fall' and 'secondary collision' are both true then the only possible outcome is outcome 12, regardless of the occurrence of other events. The resulting model is logically identical to one in which the consequence NPT is fully quantified, but can be produced much more quickly.

Appendix B1 shows that the BN calculates the same accident consequence probabilities as the original event tree of Figure 28. The consequence NPT is too large to show in the diagram.

7.3.2 Undefined event outcomes

If the 'open track' event tree was fully expanded, as is the case with the event trees shown in Figure 27, it would have 128 different consequences. However in some instances, if it is known that a subset of the events has occurred the final consequence can be determined. For example in Figure 28, if it has been established that: 'contained' = No, and 'clear' = Yes then it is certain that the outcome is consequence number 2. The event tree model does not define the states of subsequent events in the tree. There are two reasons why this might be the case. The first is that the state of the event has no effect on the consequence; looking again at the path leading to consequence 2, the direction that the train derails in is irrelevant to the consequences of the accident, as it is known that the train has maintained its clearances and will not hit a structure or other train. In this thesis such events are referred to as 'don't care' events. The second reason is that whether or not the event has occurred is inevitable given the occurrence of one or more of the preceding events. For example if it has been established that the train has maintained its clearances following derailment (clear = Yes), then it is certain that the train will not fall onto its side, it will not hit any structure, no structure will collapse onto the train and there will be no collision with another train. The event tree notation does not distinguish between these different reasons for collapsing the event tree structure. Therefore in order to replicate the event tree function and calculation in a BN a model would not need to distinguish between them either.

7.3.3 Parameterisation of the BN event tree model

Next, the extension of the BN event tree model to make it more general is described. RMR2 states that the ideal UK railway risk model 'should allow all significant and quantifiable technical, operational, organizational and performance conditions that cause accidents or exacerbate risk to be explicitly modelled'. It is a simple process to

include additional conditions in the BN version of the event tree. The conditions whose states form the underlying assumptions of the initial model can be made explicit as BN nodes. The relationships between the states of those conditions and event probabilities are then elicited. The resulting model is a 'parameterised' one, in which the impact of changing conditions can be evaluated.

Table 3 listed the conditions that the risk analyst who produced the core derailment study identified as those that affect event probabilities in the core derailment study, and which were considered to be the key assumptions of the model. Therefore these were the conditions that were included in the model. Table 4 listed which events in particular these conditions influence. This information was used to expand the BN to include these conditions as nodes in the BN. Figure 30 shows the BN produced. The event nodes, previously shown in Figure 29, are shaded. The consequence node and arcs previously shown are omitted for clarity.

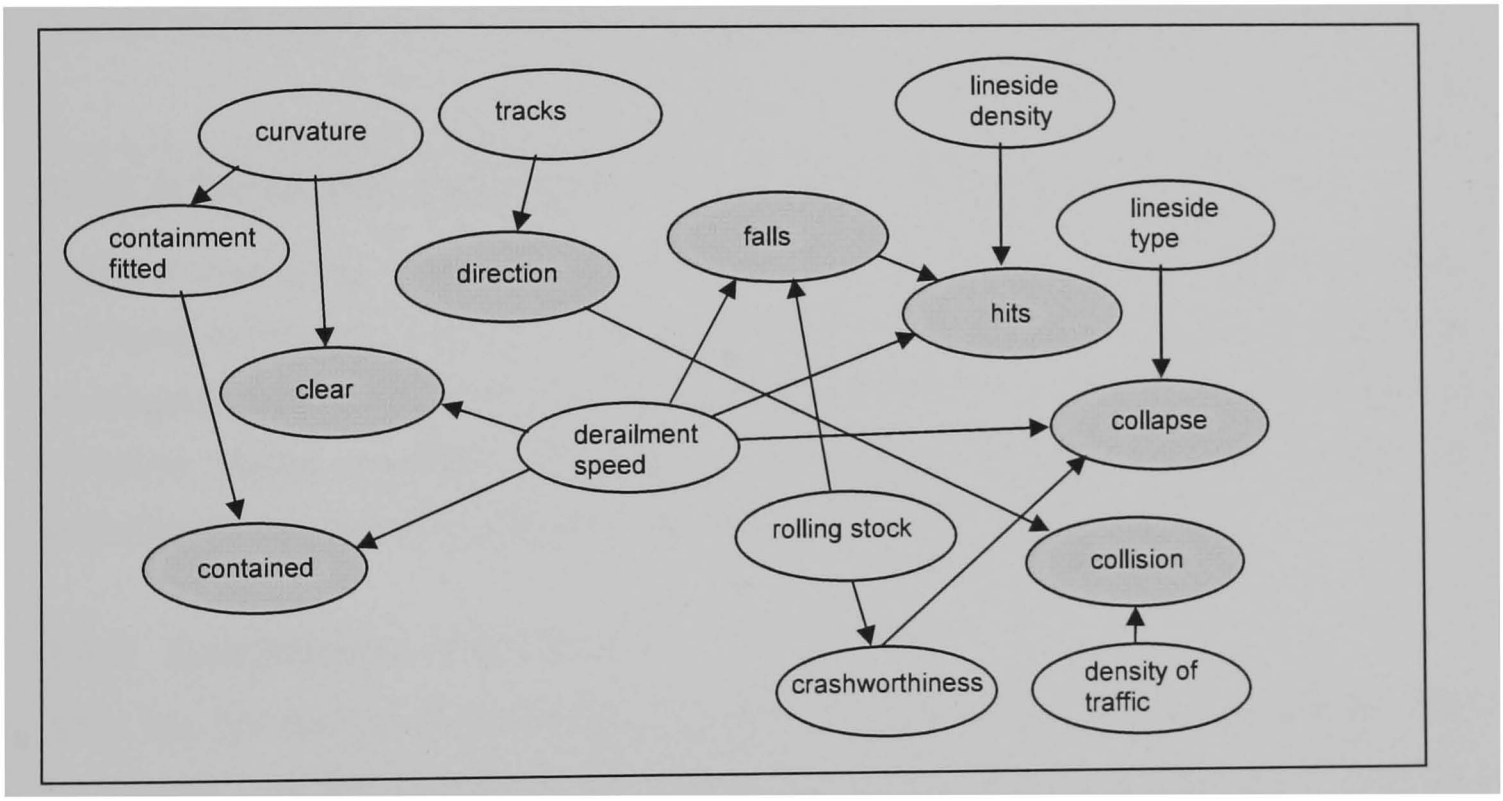


Figure 30: Parameterised 'Open track' BN event tree

The full BN structure and the set of NPTs necessary to quantify the model are shown in Appendix B2.

Condition	Condition description	Condition states
Derailment Containment Fitted	Whether the derailment containment is fitted.	Yes, No
Track Curvature	The curvature of the track	Severe, Mild, None
Number of tracks	The number of adjacent tracks:	2, 4
Derailment Speed	The speed of the derailment (mph)	>15, <15
Lineside Object Density	The density of objects beside the line	High, Low
Lineside Object Type	The type of equipment beside the line	Fixed, Anchored
Density of Traffic	The traffic density	High, Low
Train Crash Worthiness	The crashworthiness of the train	High, Low
Rolling Stock Type	The type of rolling stock	High Speed Train, Electric Multiple Unit

Table 6: Derailment operating and infrastructure conditions

Table 6 shows the conditions that were modelled and their states. Note that only technical conditions and performance conditions are modelled, as these were the conditions that were identified by the risk analyst. For this case study the number of condition states modelled was kept to a minimum to minimise the number of probabilities that needed to be quantified in the NPTs of the resulting BN.

7.3.4 Quantification of the model

After the BN had been constructed, all NPTs had to be produced or updated. The conditional probability relationships in the 'open track' event tree were used in the first instance. Table 5, listed the condition states that were previously identified as being relevant to the 'open track' event tree. These condition states reflected the fact that the core derailment study concerned a high density urban commuter railway (see column 1 of Table 7).

BN variable	Core Derailment study assumptions (commuter railway)	Alternative assumptions (intercity railway)
Containment fitted	No	No
Curvature	Severe	None
Tracks	4	2
Derailment speed	>15mph	>15mph
Lineside density	High	Low
Lineside type	Anchored	Fixed equipment
Rolling stock	EMU	High Speed Train
Density of traffic	High	Low

Table 7: Values entered into the BN Event tree model

The NPTs of the condition nodes were quantified so that, with these condition states entered, the event probabilities in the BN were identical to those in the 'open track' event tree. This ensured that the BN event tree that was produced by entering the core derailment study assumptions calculated exactly the same output as the original event tree. It can be seen from Table 7 that, for the core derailment study 'open track' event tree the density of traffic is 'high'. In the 'open track' event tree in Figure 28, It can be seen that the probability of collision in the event tree is 0.1. Therefore this value is used to quantify the BN as shown in Table 8.

Collision				
Density of Traffic	high		low	
direction	cess	adjacent	cess	adjacent
False	1	**0.9**	1	0.99
True	0	**0.1**	0	0.01

Table 8: NPT for the event node 'collision' in the parameterised BN event model

The additional conditional probabilities necessary for completing the NPTs (shown as greyed out text) were elicited with the help of the risk analyst who developed the initial study. The presence of the initial probability values in the NPTs simplified elicitation of the remaining probabilities needed to complete the NPT by providing a value for comparative purposes. Table 8 shows that if the train derails to the cess a collision is impossible regardless of the density of traffic. When the train derails to the adjacent line the risk analyst considered it 10 times less likely that a collision would occur when traffic density was deemed to be 'low'. The BN model was built using the Hugin software package.

7.3.5 Investigation of the model output

The parameterised model produced in this section is capable of representing a set of different open track event trees. Moreover, it makes the reasons for variability in event probabilities explicit. To illustrate this, different evidence was entered into the condition nodes so that the model was representative of derailment risk in an entirely different infrastructure area: an inter-city traffic area. To do this, the evidence shown in column 2 of Table 7 was entered.

When this evidence was entered, the likelihood estimates for each of the possible derailment scenarios changed significantly. This can be seen in the diagram of Figure 31. The full table of results is shown in Appendix B2.

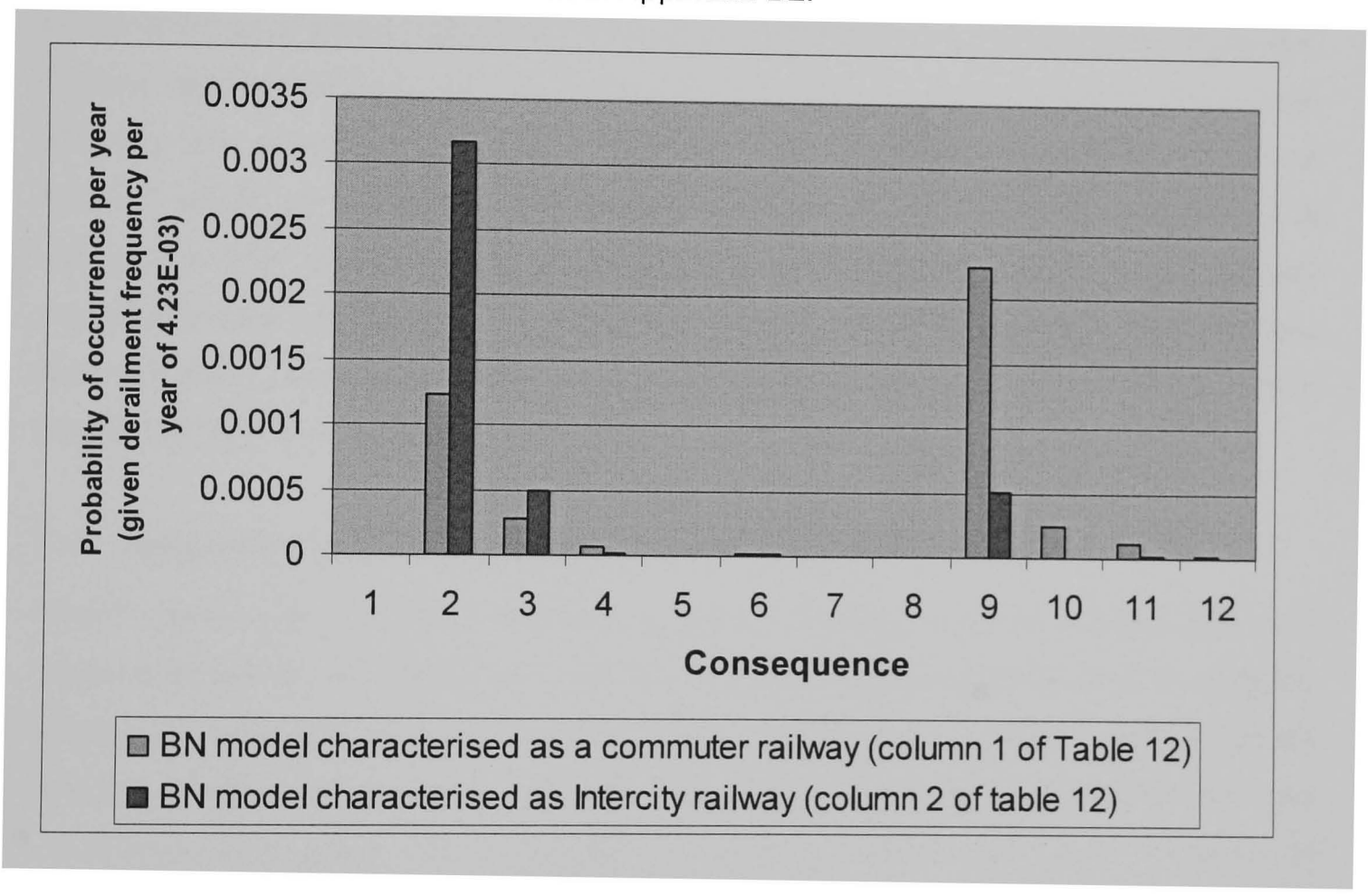


Figure 31: Accident probabilities for two scenarios calculated using the BN

Figure 31 shows that changing the states of variables in the BN has a significant effect on the likelihood of each possible consequence following a derailment. Scenario 2 (Minor derailment within clearances) is much more likely on an inter-city railway than on a commuter railway. This is because the track on the inter-city railway is much straighter, and therefore following a derailment trains are not likely to veer sharply off course and travel outside of their clearances. For the commuter railway the most likely outcome is Scenario 9 (minor derailment to adjacent line) as the track curvature is assumed to be severe and therefore clearances are not as likely to be maintained following a derailment. Also the commuter railway is a four-track railway, and therefore it is quite likely that any derailment will be towards an adjacent line. It should be noted

that, in this case study, it was assumed that traffic on the intercity infrastructure had the same speed profile as that on the commuter railway. Modelling speed changes would have entailed a more detailed probability elicitation process. This means that changes to the probability of occurrence of derailment consequences occur only because of differences in the infrastructure, type of rolling stock and traffic density.

The probability of occurrence of a derailment was taken from the core derailment study and is set at 4.23E-03 derailments per train mile per year. Because the scope of this model does not include the causes of derailment, this value is the same for both the commuter and intercity scenarios. In other words the consequence probabilities (c1 to c12) sum to this value for both modelled cases. In reality however, it is known that the states of some of the conditions influence the probability of occurrence of a derailment. Table 4 highlighted that both the extent of track curvature and the speed of the train influence the probability of a derailment. Therefore, to improve the accuracy of the model it would be necessary to expand its scope to look at derailment causes. This indicates a need to expand the model into the causal relationships that are traditionally modelled in fault trees (how to do this is investigated in the next chapter). Nevertheless the case study clearly illustrates the dependence of event tree results on the condition states that form their assumptions.

7.4 Parameterisation of a Multiple Event Tree BN

RMR3 states that an ideal modelling approach should result in models that are: 'parameterised by conditions so that the risk at different locations and in different situations on the railway network can be rapidly recalculated'. This is partially achieved with the model described in the previous subsection. The model is parameterised and various condition states can be set within it to model different situations. However its application is limited by the fact that it is based on the 'open track' event tree. The BN produced cannot model the accident risk arising on any areas of track where additional events, that are not possible on open track, might occur.

I now investigate how to create a model which can be used to model the probability of occurrence in a wider range of locations. This is done by combining the information, and event branching logic from the full set of event trees produced for the core derailment study and hence a large set of possible events.

7.4.1 Translation of several event trees into a BN

The first step in the development of the multiple event tree BN is to build a large 'extended' event tree that includes all of the events in all of the individual trees. Starting

with such a tree, it is possible to scope it to represent any of the individual trees on which it is based just by altering event probabilities. For the sake of simplicity, and to demonstrate the methodology five of the six event trees from the core derailment study are merged in this example. The five event trees used are shown in full in Appendix A. The event tree modelling derailments on bridges is omitted because it has a fundamentally different structure. It could be included using the same method, however by restricting the example to the five other locations a clearer illustrative example of the approach is achieved. Figure 32 shows the resulting merged event tree which describes the logical structure of the BN.

The event tree is very similar to the open track event tree shown in Figure 28, the only difference being that this event tree contains an additional event 'hit tunnel'. The presence of this additional event leads to two additional consequences 3 – 'major derailment to cess, tunnel portal hit' and 10 – 'major derailment to adjacent line, tunnel portal hit'. Insertion of these additional consequences leads to the renumbering of the consequences from 1 to 14 as shown on the diagram. The events in the event tree are a superset of the events that are present in all five event trees from the initial study. The event tree model could be thought of as a model of the 'top logic' of the set of event trees used in the core derailment study.

To transform the event tree of Figure 32 into the event tree of Figure 28, the appropriate probabilities of occurrence are added to each branch of the tree. 'Hit tunnel' cannot occur in the open track event tree. Therefore the P(strike tunnel portal) is set equal to zero in both of the branches in which it occurs. This indicates that collision with a tunnel is not possible in areas of open track where there are no tunnels and makes consequences 3 and 10 impossible. Hence the resulting tree becomes mathematically identical to the event tree of Figure 28. A similar approach could be applied to the event trees for each of the five locations.

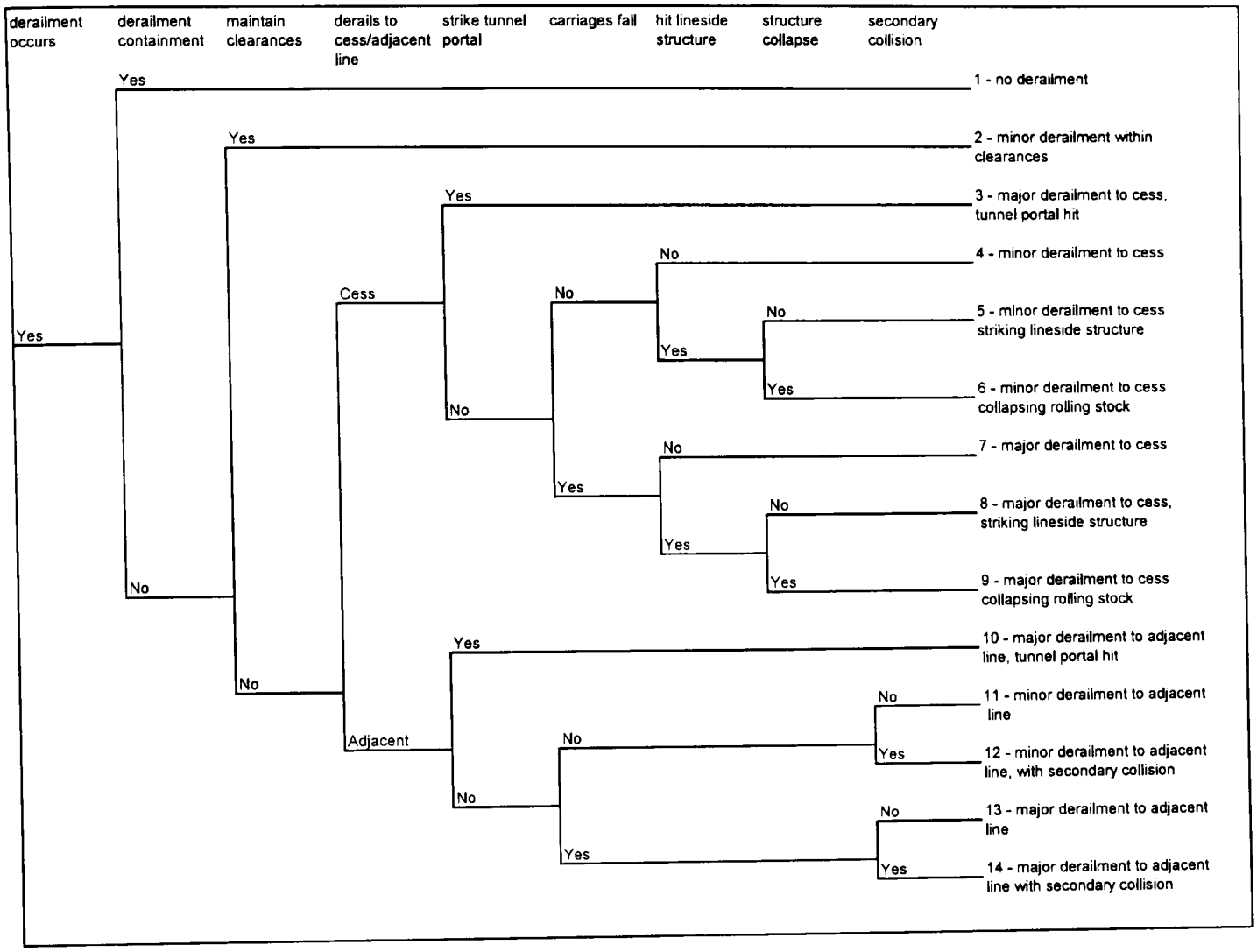


Figure 32: 'Extended' event tree showing all branching logic

To automate this process in the BN an additional node 'location' is created to update event probabilities according to the location of the derailment. This node has one state for each of the event tree locations: 'open track', 'station', 'twin track tunnel', 'through station' and tunnel approach'. The BN model produced is shown in Figure 33.

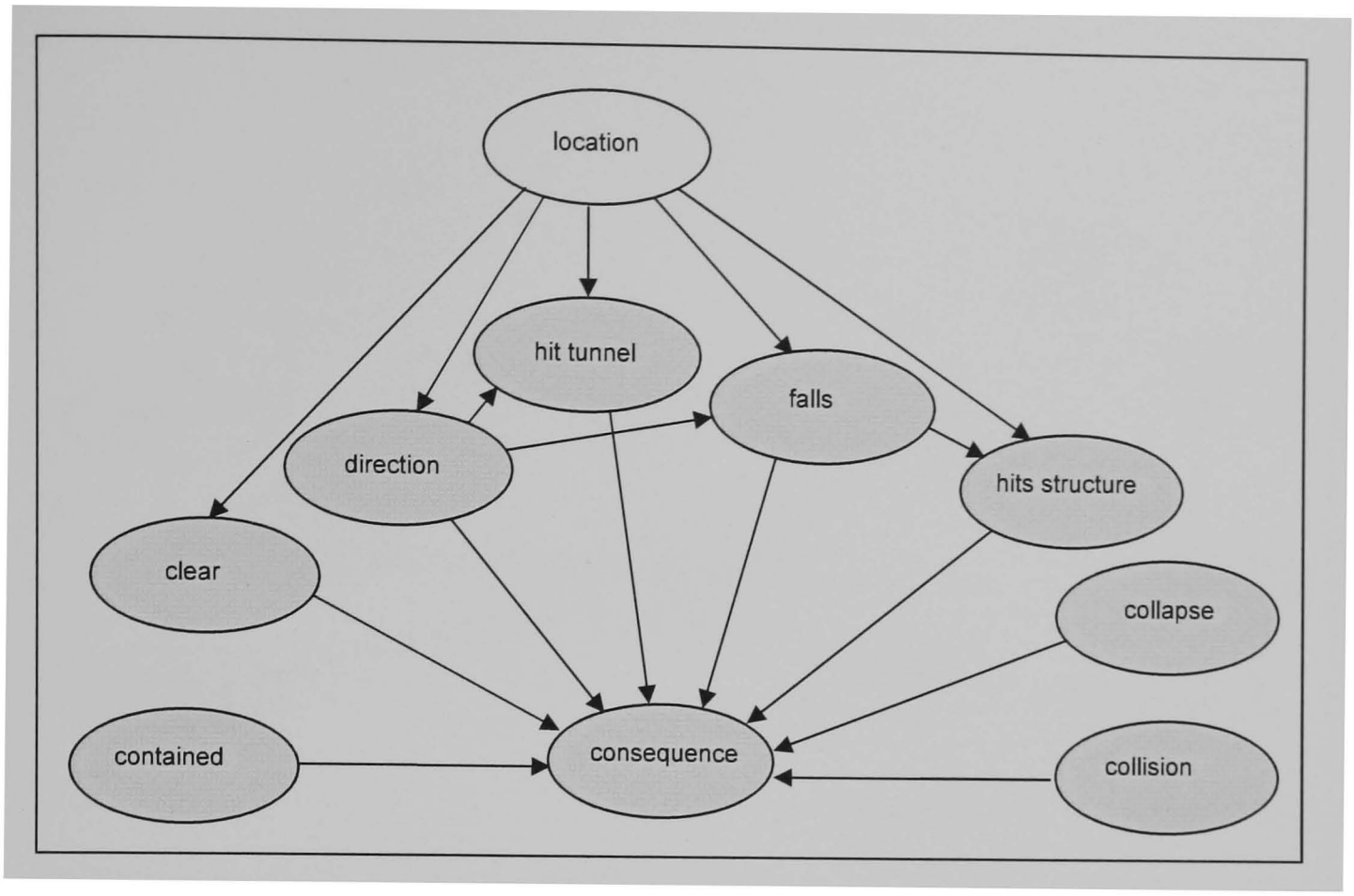


Figure 33: BN event model representing five related derailment event trees

The model must be capable of representing all conditional probability relationships between events in each of the original event trees. Links between events are added if they are implicit in the probabilities assigned to any of the individual event trees. Therefore the arc between 'falls' and 'structure' that was shown in Figure 29 is also shown here. Note also that there is an arc shown between events 'direction' and 'hit tunnel'. This is necessary to capture a conditional probability relationship present in the 'tunnel approach' event tree which exists to represent the fact that a train is more likely to hit the tunnel on the cess side as the tunnel is closer to the train on this side. Some nodes have no additional conditional dependency relationships ('contained', 'collapsed' and 'collision'). This is because their probabilities of occurrence are identical in all event trees and are not dependent on either the location in which the derailment occurs or on the occurrence of previous events.

7.4.2 Additional elicitation: adding variable assumptions

In order to generalise the model, the same variables as were used previously to generalise the 'open track' model were introduced and probability relationships elicited. The resulting model is shown in the diagram of Figure 34. Again the consequence node and arcs are omitted for clarity.

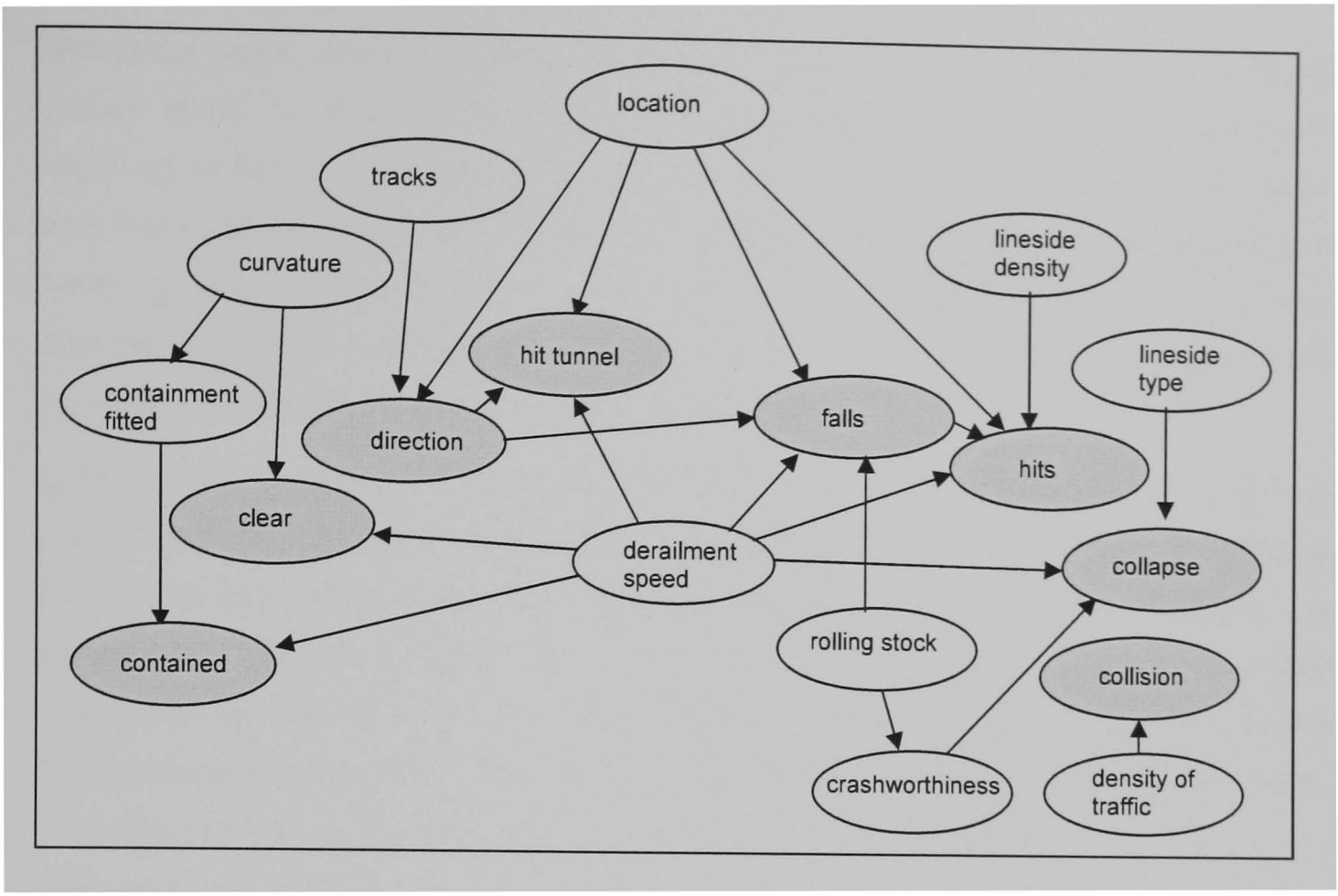


Figure 34 Parameterised BN event tree model of five merged scenarios

The full BN structure and the set of NPTs necessary to quantify the model are shown in Appendix B3.

Note that the conditional probability arc between 'location' and 'clear' that was shown in Figure 33 is not present in the parameterised model. This is because it has become redundant in the parameterisation process. Table 9 shows the NPT used for the node 'clear' in the initial BN model shown in Figure 33.

Clear					
derailment location	**open track**	**station**	**twin track tunnel**	**Through station**	**tunnel approach**
Yes	0.29	0.375	0.29	0.29	0.29
No	0.71	0.625	0.71	0.71	0.71

Table 9: NPT for the node 'clear' in Figure 33

The values in this NPT are simply transcribed from the probabilities of occurrence of the event 'clear' in the event tree for each separate location indicated. The NPT shows that the probability of a derailed train maintaining its clearances is 0.29 in all locations except for in stopping stations, where it is 0.375.

While undertaking the elicitation process, the risk analyst confirmed that the probability of 'clear' is determined by the speed at which the derailment occurs and the degree of track curvature. Track curvature was assumed to be high in all locations on the core

derailment study. However, speed differs according to location. A train in a stopping station would be likely to be travelling at low speed, and hence any derailment occurring in this location would be likely to be a low speed derailment. A low speed train would be more likely to maintain its clearances and this means that probability of 'clear' at this location is higher than that in other locations. The location of the derailment in fact provides an indicator of the state of 'derailment speed' and 'curvature' which are the real conditons of interest.

In the parameterised BN model, 'derailment speed' and 'curvature' are included as nodes. This allows use of these nodes, rather than the 'location' node, to explicitly model the key relationships that determine whether or not a train maintains its clearances. The NPT for 'clear' that is required in order to quantify the parameterised model is shown as Table 10. The two values taken from the derailment study (0.29 and 0.375) are entered into the table first, according to the assumptions that underpin them. The other values were elicited with the assistance of the risk analyst.

Clear						
derailment speed	**>15**			**<15**		
Curvature	**severe**	**Mild**	**None**	**severe**	**Mild**	**None**
Yes	**0.29**	0.6	0.75	**0.375**	0.7	0.9
No	**0.71**	0.4	0.25	**0.625**	0.3	0.1

Table 10: NPT for the node 'clear' in Figure 34

In this NPT, there is no need to repeat 'clear' occurrence probabilities, as was the case in the previous NPT shown in Table 8. In fact, in many cases the location of the derailment does not in itself determine the probability of occurrence of each event. Instead, the location indicates the state of local conditions that do directly influence the events. If the model is fully parameterised such that all these conditions are made explicit, then the 'location' node would no longer be needed.

Note that using a standard event tree approach the calculation of the severity of accident outcomes is undertaken externally to an event tree. However, some conditions included in the model such as train speed and crashworthiness impact upon the severity of accident outcomes. Using the BN approach outlined here, condition states set in the BN model could therefore be checked for consistency with their use in severity calculations.

It should also be noted that, although the core derailment event tree scope did not include any track for which containment rail was fitted, it was possible to include for this

possibility because it is known that there are some parts of the UK network where containment rail is fitted, and that containment rail can prevent the occurrence of a derailment. To build a model that is capable of analysing risk across a network area using this approach all of the event sequences that could arise on that section of the network and the full set of events that might occur need to be able to be postulated.

7.4.3 Model validation

To validate the final BN model, the assumptions underpinning the core derailment scenario (see column 1 of Table 7) were entered into the BN, and results calculated for each of the locations in turn. This confirmed that the model gave the same results as the equivalent event tree for each location.

7.5 Use of the model

The final parameterised BN Event Model produced allows calculation of the risk in each of the locations modelled in the original study. However, the additional flexibility provided by parameterising the model by its conditions means that it can also be used to estimate derailment occurrence rates with a range of other condition states set. For example, the effect that the variation of condition states has on the derailment occurrence probability on a section of the network can be quickly and easily investigated using the model.

Note that evidence is only entered into condition nodes. The user cannot assert that events are true. This is because of the 'don't care' states mentioned in section 7.3.2. It is not known what these outcomes are, therefore the conditional probability relationships between these events and other nodes in the BN cannot be coded. Each condition node must also be set to a particular state. No prior probabilities are set on condition nodes and therefore failing to set these nodes to a particular state would result in the scope of the analysis being undefined. Some arcs are included between nodes to capture the conditional probability relationships between them. If condition states are set to values that are not consistent with these causal relationships then the BN software will flag this inconsistency, so this serves as a partial validation of condition sets entered.

Probabilities were calculated using the condition sets that supported the core derailment study, and then recalculated when one or more of the condition states had been changed. The data entered and the output probabilities calculated are shown in Appendix B3.

One of the most significant effects found was the effect of track curvature on derailment outcome probabilities. The graph of Figure 35 shows BN event model calculation results for a commuter railway with severe track curvature, and one with no curvature at all.

The graph shows that when track is straight derailed trains are much more likely to maintain their clearances. There is approximately an 80% chance that if a train derails on a straight section of track it will stay within its clearances. This mirrors the findings shown in graph of Figure 31, as the degree of track curvature was a significant difference between the commuter and intercity railway infrastructure.

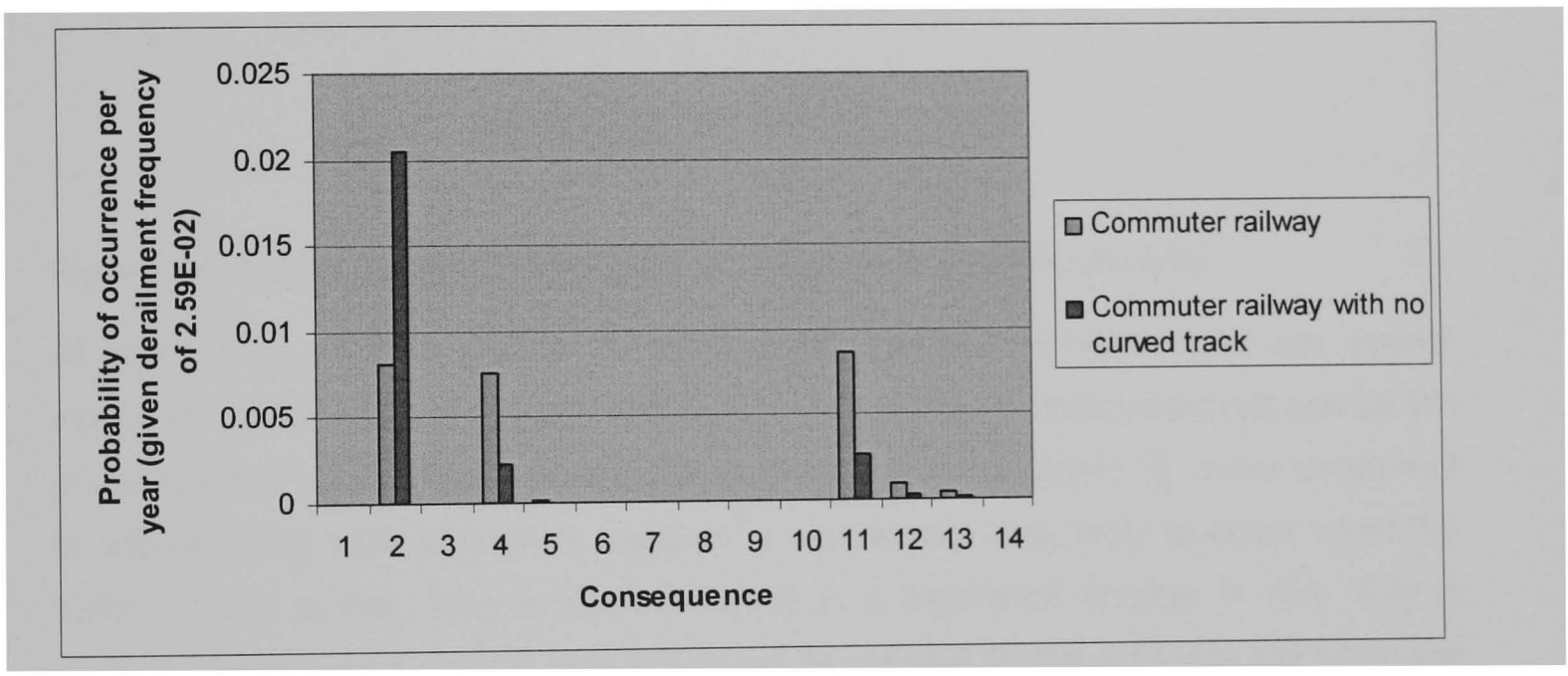


Figure 35: Model output: severe track curvature, and no track curvature

Another effect investigated was how traffic density affects the consequences of a derailment. The graph of Figure 36 compares calculation results for a commuter railway with high traffic density, and one with low traffic density.

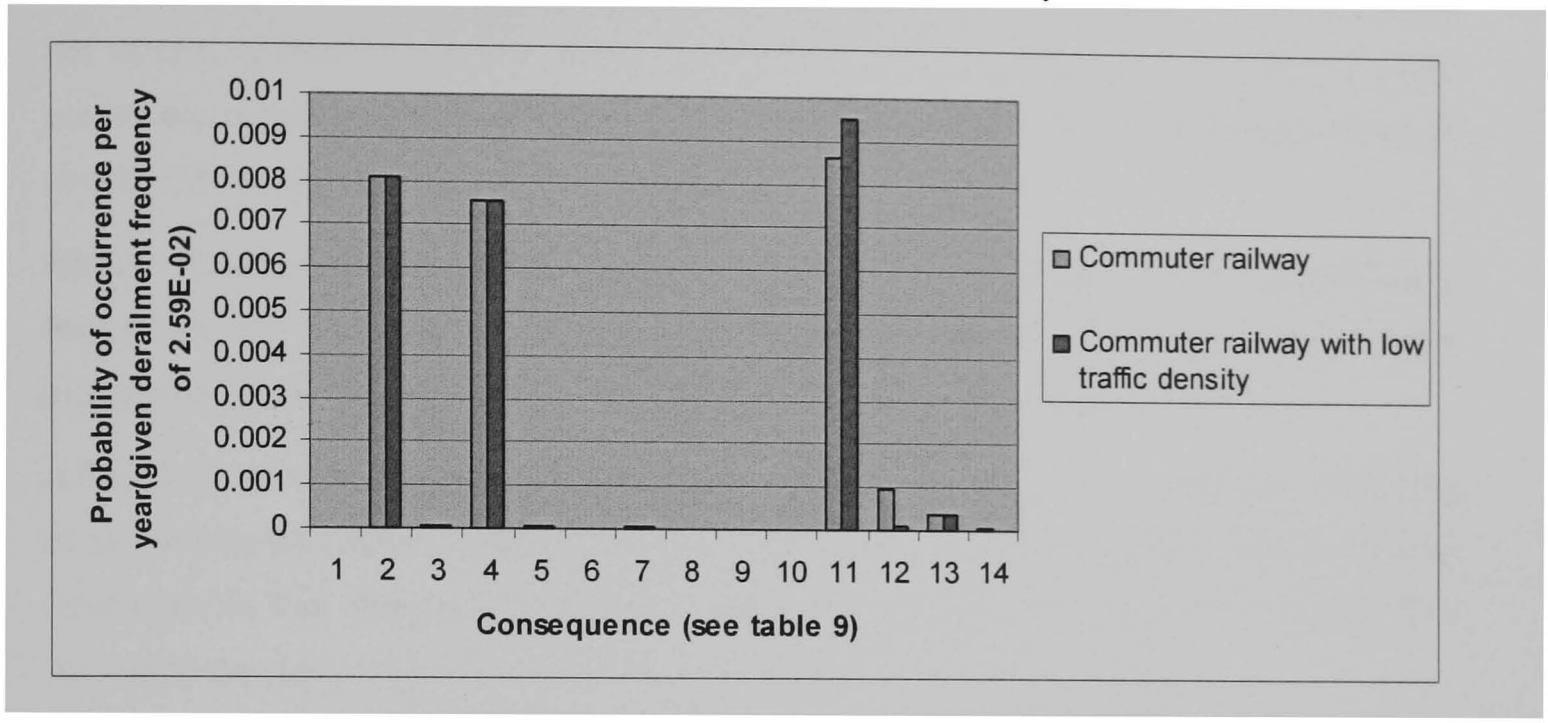


Figure 36: Model output: high traffic density and low traffic density

At first glance, the difference in the two consequence profiles does not appear significant. However it should be borne in mind that risk is determined not just by the probabilities of each consequence but also their severity. Accident 12 'minor derailment to adjacent line, with secondary collision' is significantly less likely to occur when the traffic density is low. This is likely to result in a significant change in risk. This is because there is less chance that a train will be present on the adjacent line when the derailment occurs. In order to determine the degree of risk reduction that is achieved by this reduction in traffic density, further calculation must be undertaken externally to the model.

7.6 Review of the model

The parameterised BN model produced at this stage meets some of the ideal requirements for railway risk models highlighted in section 4.3. At this stage, a full modelling methodology has not been developed. However, the model is reviewed to assess its potential as an approach and consider any areas requiring further investigation and development.

7.6.1 Review against ideal risk modelling requirements

In this section, the model is reviewed against the ideal risk modelling requirements previously set out.

RMR1: Risk models should allow as many of the events in an accident sequence to be modelled as is practicable.

The model described in this section includes some events in the accident sequence but not others. It uses the same event tree models as the SRM and the industry study previously mentioned and is therefore concerned only with the possible sequences of events following the occurrence of a hazard.

RMR2: Risk models should allow as many of the significant and quantifiable technical, operational, organizational and performance conditions that cause accidents or exacerbate risk to be explicitly modelled as is practicable.

A fundamental requirement of the desired approach is that it should allow the modelling of conditions and their possible states of existence as well as events. The BN model developed in this chapter shows how it might be possible to build such a model. The approach can be used to make conditions explicit as nodes in the BN.

Standard event tree notation does not allow the underlying conditions to be modelled. Therefore the conditions that underpin the event trees need to be carefully documented as assumptions. As was found in section 4.3, even the most diligent of analysts might forget to record an assumption or miss the effect that varying it has on an event elsewhere in the model. It was observed that, when conditions are manually documented it is easy to make inconsistent assumptions in various parts of the same model. During discussion with the risk analyst who undertook the original study he commented that, as each event tree was produced independently, it was difficult to consistently manage all assumptions across the set of event trees.

RMR3: The model should be parameterised by conditions so that the risk at different locations and in different situations on the railway network can be rapidly recalculated.

The BN model is parameterised by the states of conditions. There are 768 different possible combinations of the condition states shown in Table 6. The model can be set to calculate accident outcome probabilities with any of these combinations. In the initial study, only six sets of condition states were modelled.

Using the BN, a modular approach to modelling is followed. The event branching structure shown in the event tree of Figure 32 is re-used for each calculation, avoiding the need to build separate models. Output calculations can be undertaken under different conditions simply by entering condition states into the BN as evidence and propagating this information through the BN.

The core derailment study, like the SRM, uses fairly crude assumptions across large geographic areas, to reduce the need to build many multiple event trees. Simplifying assumptions in this way reduces the accuracy of the model produced, and makes it hard to establish a context for the model or the meaning of its output. For example, it was assumed that track curvature was 'severe' across the whole of the infrastructure area modelled. In fact this is a crude assumption. The analyst confirmed that only up to 80% of the network is either 'severely' or 'moderately' curved, with the remaining 20% being straight track. The assumption that all track was severely curved meant that known information about the infrastructure was ignored because it was considered to be too difficult and time-consuming to include. As the investigation into the effect on risk of varying the assumptions of the study shows (see Figure 35), the degree of track curvature can have a significant effect on risk. Using the BN model, a true understanding of the states of conditions can be modelled rather than making such assumptions. The accident outcome probabilities can be calculated in each circumstance and then aggregated to a network total by considering exposure data – the number of track miles relevant to each set of conditions.

The approach has other benefits. As part of the original study, the analyst undertook a sensitivity analysis to determine how sensitive the model output was to the states of various conditions. To do this, it had been necessary for him to construct additional event trees. He stated that this was a time consuming process that acted as a discouragement against undertaking such analysis. He noted that the BN model allows such sensitivity analysis to be undertaken simply by altering the states of conditions. This would make it much easier to undertake sensitively analysis making it likely that it would be done more thoroughly.

7.6.2 Areas requiring further investigation and development.

Some of the condition states that are made explicit in the BN model influence derailment occurrence rates. For example, the analyst stated that 'track condition' and 'track speed' influence the probability of a derailment (Table 3).

In this model the events in the accident sequence that precede the initiating event of the event tree are not modelled. If a model was produced that did include such events it would be able to model correlations between these events and the events modelled in the event tree easily. This would resolve the potential lack of coherence associated with bow-tie models.

To do this the BN model needs to be expanded to include:

- the various events that precede the occurrence of the event tree initiating event.
- all conditions that influence events anywhere in the accident sequence
- the conditional probability relationships between all events and conditions modelled.

In the next chapter a model of this type is described.

7.7 Chapter Summary

In this chapter, I have shown how to develop BN models that are functionally equivalent to event trees, using clear repeatable rules. Using a train derailment case study, based on an existing industry analysis, I have also shown how a number of related event trees can be combined into a single BN model. This is achieved by developing an extended event tree, containing all possible events from a set of related event trees, and applying the translation rules developed.

The probabilities of occurrence of events in an event tree are dependent on the state of a number of conditions. The BN models produced are 'parameterised' by making these condition states explicit in the model, and eliciting additional conditional probability relationships. This process was undertaken with the risk analyst responsible for the original report. This process produces a more general model which can be used to calculate the same output as the original trees but can also be used in a wider range of circumstances.

The resulting model possesses some of the properties that were outlined as necessary for risk models in the railway industry allowing the rapid update of assumptions, and recalculation of model output to adapt the model to represent different locations, or situations and run calculations to see how the accident probabilities are affected.

However, there are a number of difficulties that remain to be overcome to use this technique to build dependable risk models. In particular BN models of this type are based on the assumption that initiating event occurrence rates are constant regardless of the particular condition states that are entered into the BN. This assumption is not considered to be a valid one, as condition states may affect the probability of hazard causes as well as events. The next chapter describes an expansion of the approach to address this point. The method described involves the combination of the BN event tree model with BN equivalents of fault trees. Both models are parameterised and common parameters are shared between the models.

8 Case Study Part 2: A parameterised risk model

In this chapter, I outline part 2 of the case study which builds on the work described in part 1 (Chapter 7). The approach is extended to develop a parameterised BN model which incorporates the events preceding the initiating event of the event tree. Like the event tree based model described in the previous chapter, the model is based on a standard causal modelling approach that models logical event sequences: fault tree analysis. The fault tree model is similarly parameterised by making condition states explicit and variable and is quantified using available data and expert judgement.

The key features of models of this type are described, and I argue that these features substantially meet the ideal requirements for risk modelling RMR1-RMR3 that were previously set out. This argument partially supports Hypothesis 4, that models which meet the ideal requirements were set out are possible.

8.1 Conceptual overview of the parameterised risk model.

The diagram of Figure 37 shows a conceptual outline for the type of risk model that is proposed in this chapter. The outline shows the structure of the model, and its distinct parts, and provides reference to subsequent sections of this chapter which describe the model in more detail.

The model consists of sets of BN nodes and arcs representing:

- sequences of events which lead to different outcomes, given the occurrence of a hazard. The structure of this part of the BN encodes the logic from a set of related events trees. This part of the model was described in the previous chapter and is discussed further in section 8.2.
- the events which can lead to the occurrence of a hazard and the combinational logic by which this hazard might arise. The structure of this part of the BN encodes the logic from a set of related fault trees and is described further in section 8.3.
- the relative frequency of fault types (described further in section 8.5).
- the conditions which affect the probability of occurrence of:
    - base events in the fault tree (see section 8.4).
    - events in the event tree (see section 8.2).

In some cases, these conditions introduce correlations between the two distinct parts of the model (see section 8.6).

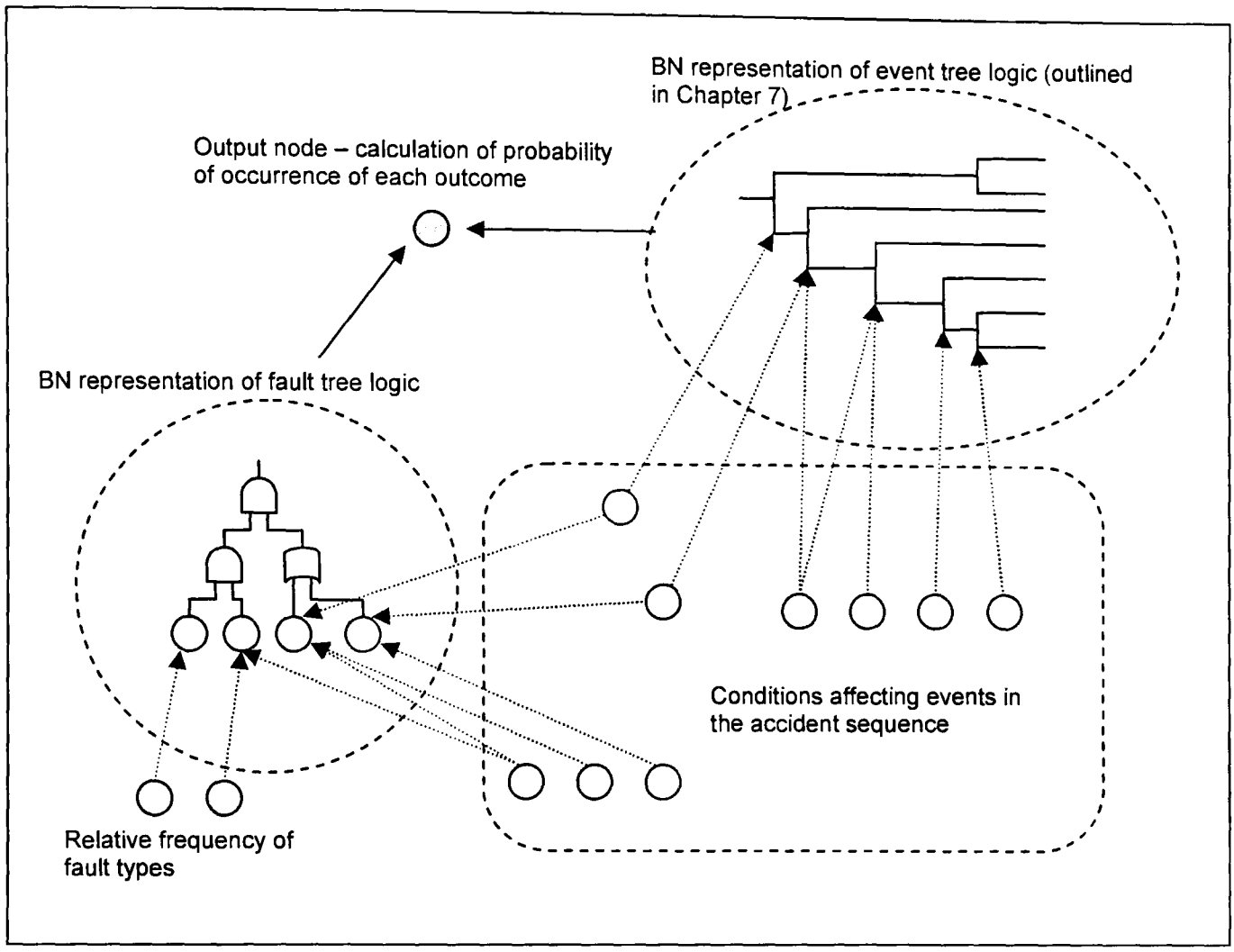


Figure 37: The structure of the complete risk model

The model also includes an output node, which calculates the probabilities of occurrence of each derailment outcome, using information from the top event of the BN fault tree and the outcome node of the BN event tree. This is described further in section 8.7.

A prototype BN model of this type was developed to estimate the probability of occurrence of a range of derailment accidents that might occur across the UK railway network. The model was developed entirely using Hugin BN software. The full model, with details of model scope, and supporting documentation and information is described in Appendix C.

8.2 BN representation of event tree logic, and conditions

The event tree logic in the parameterised BN derailment model described in this chapter is identical to that used in the event tree model described in the previous chapter (see Figure 32). However, a smaller set of conditions is modelled, including only:

- containment fitted

- track curvature
- line speed – this is considered to be closely correlated to the actual train speed
- number of tracks
- lineside object density
- lineside object type
- location of track

As will be described in section 0, the parameterised BN was produced using Hugin BN modelling software and NPT probabilities needed to be elicited and manually entered into the model. The more conditions, and condition states, that are modelled, the larger the NPTs that are needed. This rationalisation of conditions was undertaken to make the BN quantification process more manageable, given that the model developed here is for the purposes of illustrating the feasibility of the approach, rather than developing a model suitable for practical industrial use.

In the next chapter, I propose how the development of these types of model might eventually be supported by software to automate many of the modelling tasks. A discussion of how data collection might be scoped to enable routine and systematic quantification of node probabilities (section 9.2.5) is also presented. If this were possible then the time and effort required to develop the models would be reduced allowing larger models, with a more complete set of conditions, to be quantified more easily.

The BN model of event tree logic used for the model described in this chapter is shown in full in Appendix C.

8.3 BN representation of fault tree logic

This part of the model models the events which can lead to the occurrence of a hazard and the combinational logic by which this hazard might arise. A standard fault tree development approach is followed.

Section 7.4.1 described how, in order to build a BN model that was capable of representing a wide geographic area, an event tree that contains all of the events that might occur in different circumstances and locations must first be developed. Then, by entering condition nodes, a model is created that can be downscoped to represent a particular location. A similar approach is used with the fault tree part of the model. The fault tree part of the model was structured to include base events at a lower level of

abstraction than the SRM, because this lower level of analysis was supported by available data and previous modelling work. Fault types, and their failure rates were taken from the derailment risk model undertaken for RSSB by Risk Solutions (Campbell and Kennedy 2003). The resulting model is a type of Master Logic Diagram (see section 5.4) of the causes of derailment on the UK railway network. The fault tree for the prototype model is shown in Appendix C4. Although not comprehensive, the model captures the key causes of derailment on the UK rail network: overspeeding; track faults; Switch and Crossing (S&C) faults, rolling stock faults, and obstructions. It therefore also captures a wide range of the control measures that are used to detect, remove or prevent the various causes of derailment. Figure 38 shows a fragment of the fault tree model built, which relates to derailments caused by rolling stock faults (RSF). There are two key features to note about this fault tree, which are relevant to subsequent discussion:

- The fault tree models various conjunctions of events that could lead to the occurrence of the top event
- The fault tree base events have a logical sequence

The fault tree model shown includes a range of separate events further back in the accident sequence than the derailment itself, such as the occurrence of the faults that cause derailment (event 17), and the detection and control activities (events 19, 20 and 21). In this part of the model up to six separate events might need to occur to cause a derailment (see figures C1-C6 in Appendix C).

There is a logical sequence of occurrence of fault tree base events. EVENT 17, 'rolling stock fault occurs' can be considered to be the initiating event. The probability of occurrence of all other base events in the fault tree are conditioned on the occurrence of EVENT 17. For example a rolling stock fault cannot be detected (EVENT 19) unless a fault has occurred in the first place. The probability of occurrence of EVENT 19 is therefore conditional on the probability of occurrence of EVENT 17. Similarly EVENT 20 is conditioned upon EVENT 19.

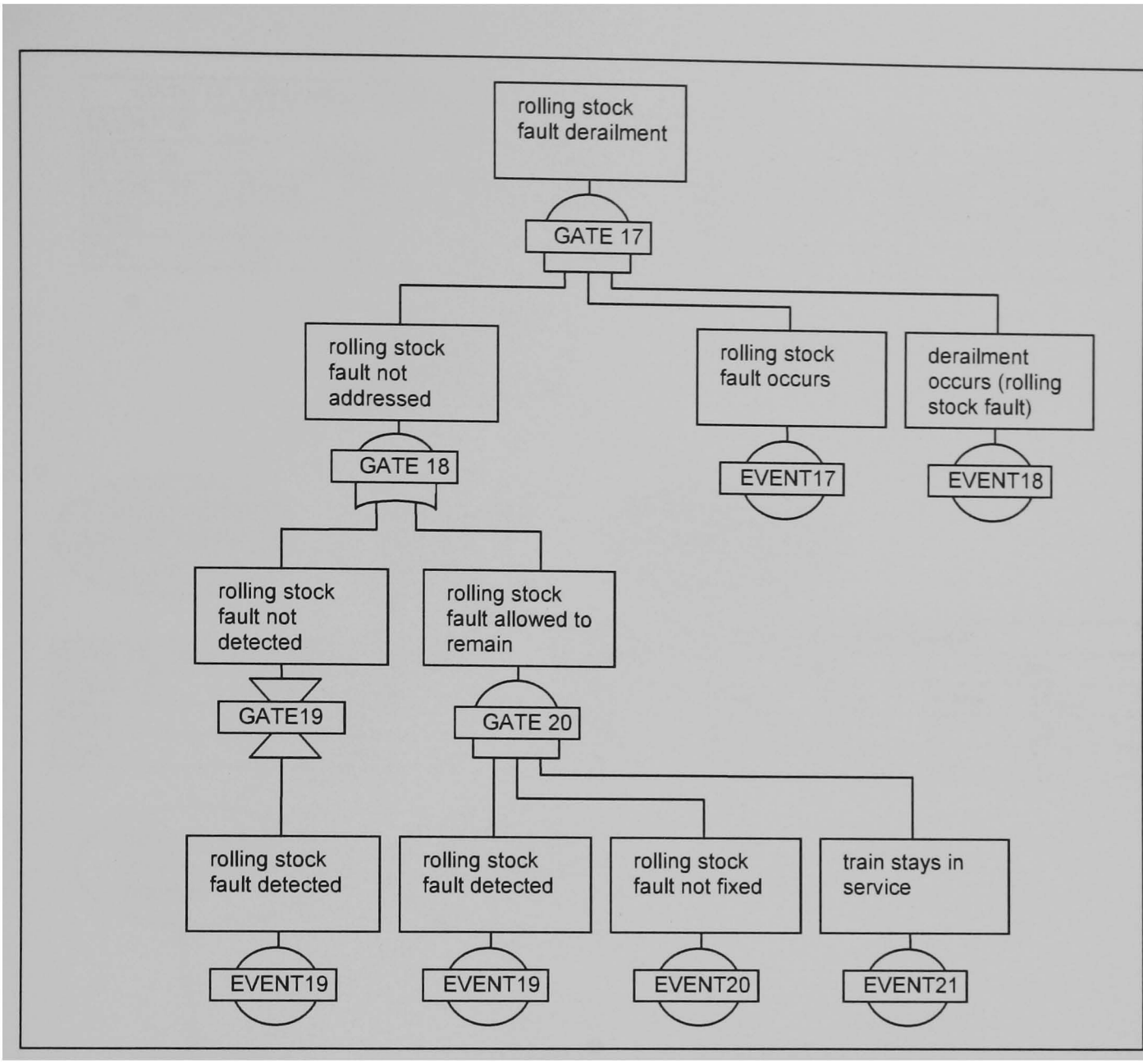


Figure 38: Fragment of the fault tree used to specify BN logic

In section 6.4.4 work by Bobbio was reviewed, highlighting the simple process by which a fault tree could be translated into a BN. The BN of Figure 39 is developed by applying those translation rules to the fault tree of Figure 38. Here, the white nodes represent gates, grey nodes represent events. The full BN fault tree model produced is shown in Appendix C4.

The NPTs for each event node have two states: true and false; and the gate nodes are quantified with NPTs probabilities as appropriate. The NPTs of the gates are simply the truth tables for the logical relationship described. The diagram shows the NPTs for gates 17, 18 and 19 which represent logical AND, OR, and NOT relationships respectively.

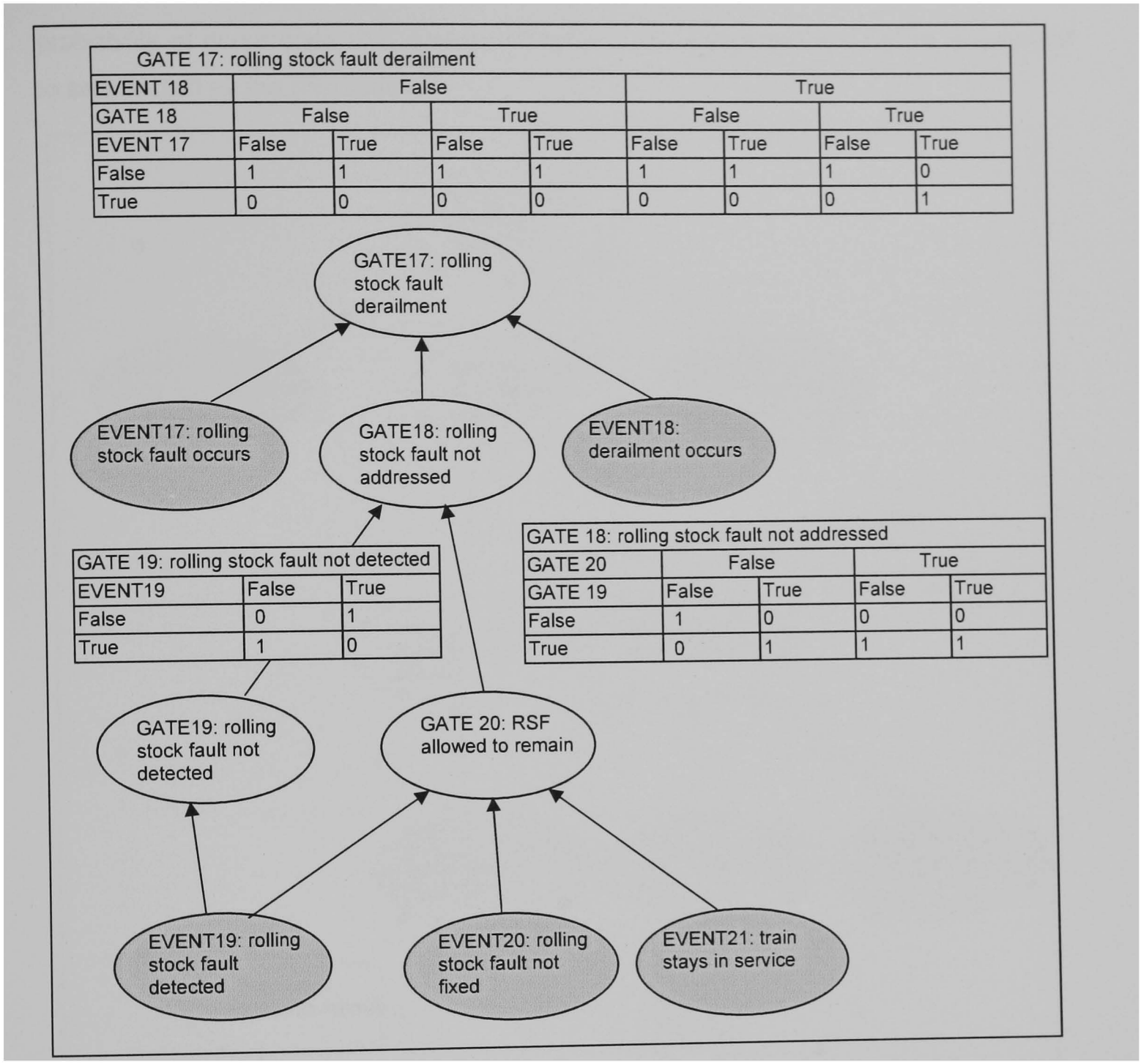


Figure 39: BN equivalent fault tree

8.4 Conditions affecting base events in the fault tree logic

In a traditional fault tree model conditional probability relationships are bound up in the definition of the base events, and by implication their coincident occurrence. For example, in Figure 38, gate 17 'rolling stock fault derailment' represents the probability of occurrence of a derailment (event 18) *given that* a roiling stock fault has occurred (event 17). This is sufficient as fault trees model the probabilities given a fixed set of underlying conditions and base event probabilities. However in the BN model, as the model must remain valid given different the existence of different underlying conditions, the conditional probability relationships must be modelled. Figure 40 shows the first step in developing such a model. It shows the BN described in Figure 39, with the addition of the condition nodes whose states influence the probability of occurrence of base events. In the BN shown dotted lines represent conditions. For example, the

probability of occurrence of a derailment (event 18, 'derailment occurs') is considered to be affected by the line speed.

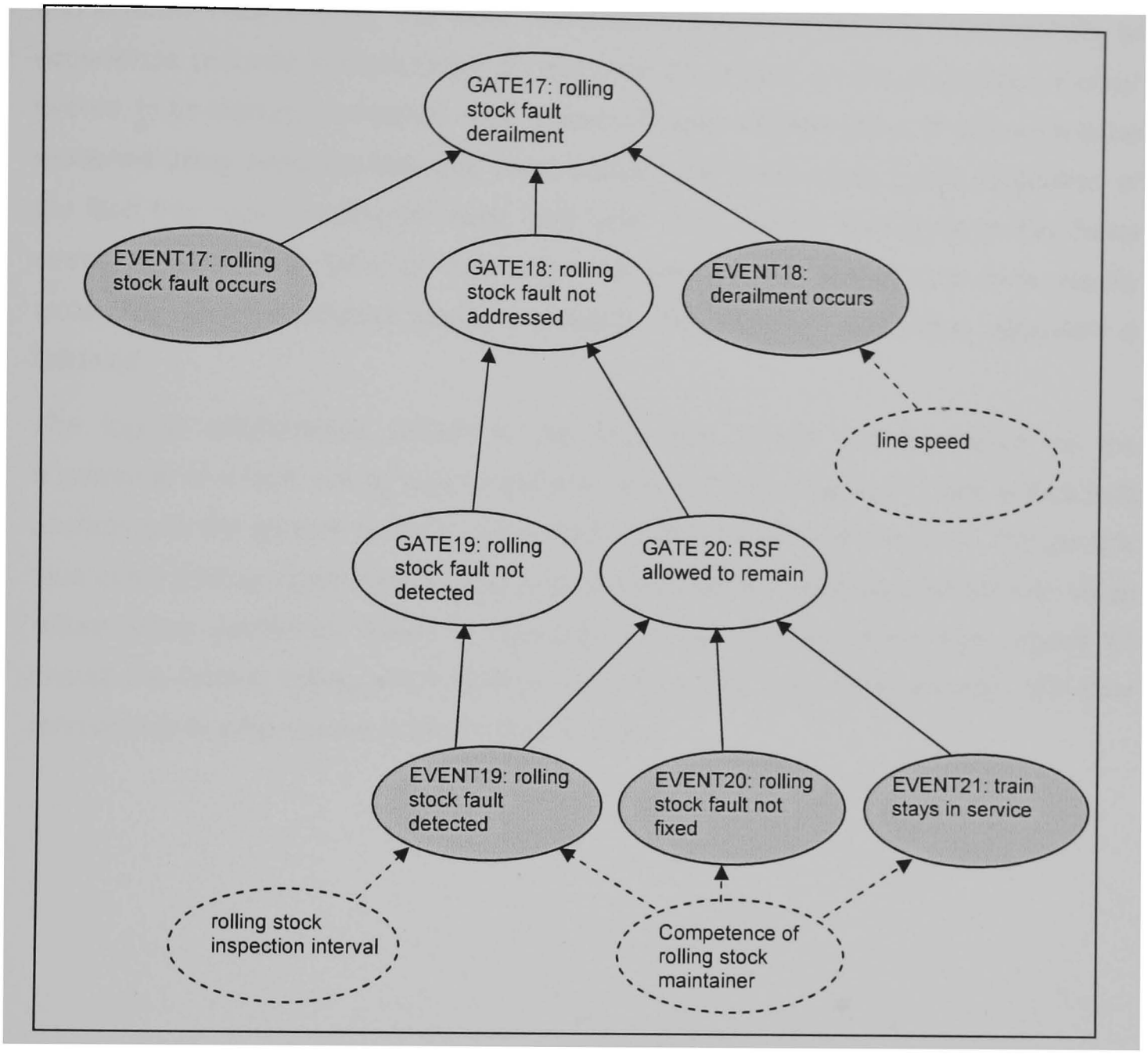


Figure 40: BN equivalent of the fault tree

8.5 Modelling the relative frequency of fault types

In section 8.3 it was stressed that there was an order in which fault tree base events would occur. EVENT 17 'rolling stock fault occurs' is the initiating event (i.e. the first of the base events in Figure 38 to occur) and this order relates to the conditional probability relationships embedded in the fault tree event descriptions. In the BN model the intent is to model a wider range of underlying conditions, and this means modelling these conditions and the conditional probability relationships. In reality there are different types of rolling stock fault that might occur, and the type and severity of rolling stock fault influences the probability of occurrence of other events in the fault tree. For example, severe failures will generally be more likely to lead to derailment but will also tend to be easier to detect. The probability of occurrence of a rolling stock fault will also

depend on the particular type of fault that occurs (for example a wheel fault and a brake fault are entirely different types of fault with different probabilities of occurrence and different implications). The ideal model would therefore allow for the probability of occurrence of these various types of fault, and the impact on the probability of other events, to be distinctly modelled. But, if each of these different types of fault were to be modelled using separate fault tree base events, this would result in the duplication of the fault tree logic needing for each fault type. The method developed in this thesis seeks to avoid this type of duplication, to prevent the model size from rapidly expanding given additional causal modelling. Therefore an alternative approach is followed.

The logical relationships shown in the fault tree model are dependent on the occurrence of a fault, not its type or severity. The fault tree logical structure is thus built according to the generic fault (a rolling stock fault in the example shown). The generic fault event (rolling stock fault occurs) is quantified with the aggregate failure rate for all failure types. Additional nodes for fault type and severity are then added. Figure 41 shows the nodes 'rolling stock fault type' and 'rolling stock fault severity' and their relationship to other nodes in the prototype model.

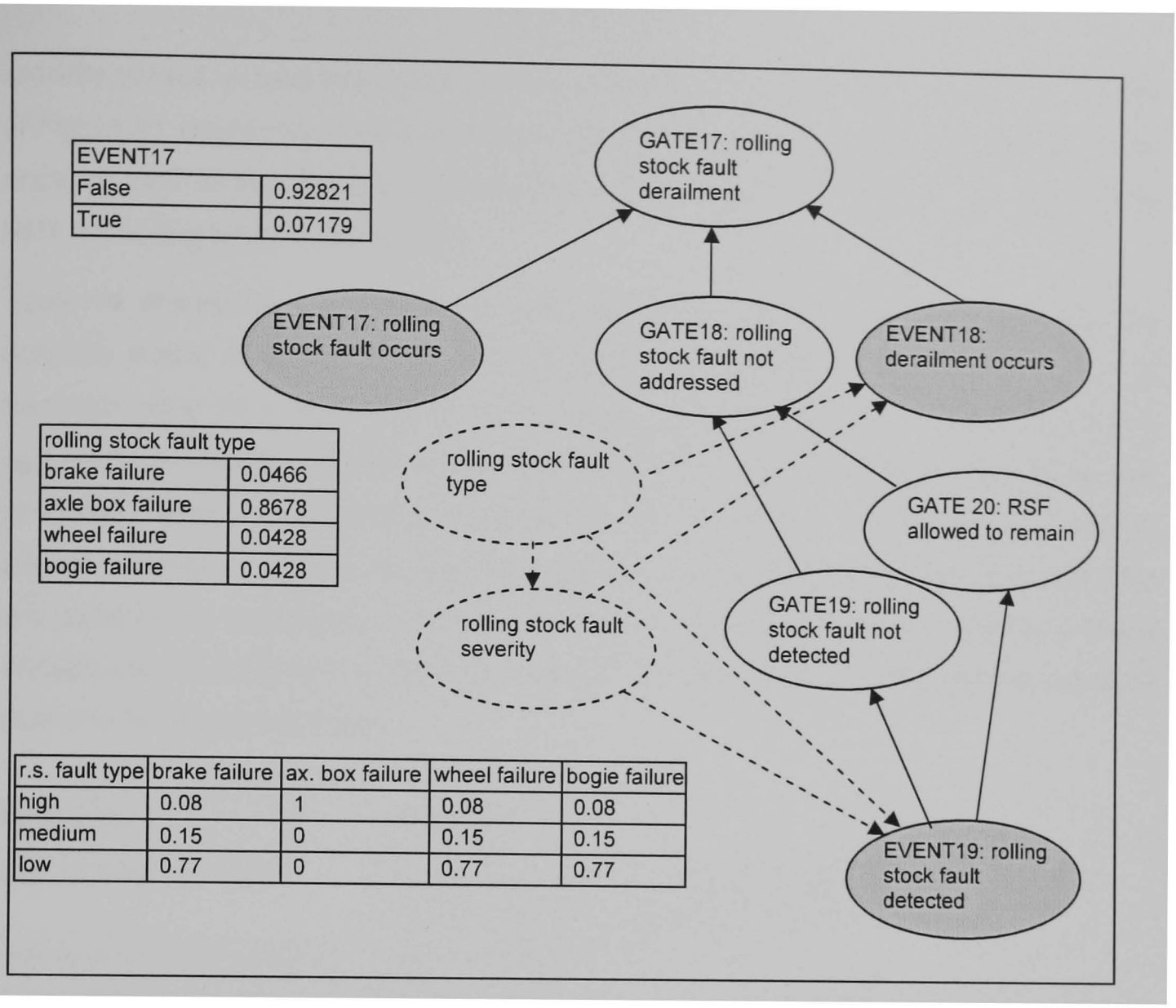


Figure 41: Nodes relating to event 17: rolling stock fault occurs

According to the fault tree logic, the top event 'rolling stock fault derailment' cannot occur unless event 17 is true. However, the occurrence of the top event is also dependent on the occurrence of other events in the model (for example events 18 and 19). The probability of occurrence of these events depends on the fault type and severity.

The model includes nodes for these factors, but these nodes are not quantified with the absolute rates of occurrence of each fault type as this information is already captured in total in the NPT for event 17. Instead, they are quantified according to the relative probability of occurrence of each of their states. For example, according to the model 4.66% of rolling stock faults are brake failures, and 8% of brake failures are of high severity. Note that the node for event 17 is not linked to either the 'type' or the 'severity' node. The link between event 17 and the fault condition nodes is in the way that they have been quantified – the absolute probabilities of occurrence for each set of fault conditions can be calculated using the aggregate total and the relative probabilities.

Using this approach, the aggregate top event probability can be calculated given all possible faults without the need to create additional models for each different type and

severity of fault. A fault tree model built to model the same sets of conditions as the BN of Figure 41 would require the fault tree logical structure to be duplicated twelve times, once for each of the discrete combinations of fault type and fault severity shown in the NPT for 'rolling stock fault severity'.

Table 11 shows the set of different fault type nodes occurring in the model and the possible states of each. These nodes are left as distributions and are not set to a particular state for a given analysis. This means that the fault tree top event gives the aggregate probability of occurrence of a derailment given all possible fault types and severities. Note that, according to the definitions in section 2.3 the fault type variables shown in Table 11 are events, and not conditions. This is reflected in the way that they are used in the model as, in common with other events, and unlike conditions these variables are not set to any particular state when using the model to develop accident outcome likelihood estimates.

fault type	**fault state**
rolling stock fault type	brake failures, axle/axle box failure, wheel faults/failure, suspension/bogie failure
rolling stock fault severity	high, medium, low
track fault type	gauge spreading, track twist, broken rail, buckled rail, subsidence/landslip
track fault severity	high, medium, low
S&C fault severity	high, medium, low
type of obstruction	engineering material, debris from lineside/overbridge, objects from trains, landslip/fallen trees, from vandals, large animals.

Table 11: Fault type variables

This approach represents a new adaptation of fault tree modelling. It allows the same logical assumptions and structure of a fault tree to be used in the BN model, but the BN approach allows a much more compact model to be built, which can calculate the aggregate top event probability of a range of different underlying base events occurrences. It also allows the specific causes which influence those base events occurrences to be explicitly modelled.

8.6 Conditions affecting base events in the BN fault tree and events in the BN event tree

There are a subset of conditions that are correlated with both event tree event nodes and fault tree base event nodes. For example the 'line speed' influences events in both

the fault tree and event tree including 'maintain clearances' and 'strike tunnel portal'. The likelihood of occurrence of both these events increases as the derailment speed increases. There are three condition nodes in the model that link the fault and event trees: 'line speed', 'track curvature' and 'location of track'. As the prototype model is constructed entirely as a BN it is a simple matter to include these correlations with the addition of BN arcs.

8.7 Output node – calculation of probability of occurrence of each outcome

The 'event tree' part of the model outputs a relative frequency of occurrence of each possible outcome per derailment. It therefore assumes that a derailment has occurred. The 'fault tree' part of the BN model which calculates the probability of occurrence of a derailment per track mile, per year. In order for the model to provide an estimate of the actual frequency of occurrence of each outcome it is necessary to conjoin the output of the two models. The parameterised BN model built here links the two output nodes of the 'fault tree' and 'event tree' parts of the model in order to calculate the probability of occurrence of each of the 14 possible outcomes per track mile per year - the absolute probability of occurrence of each derailment consequence outcome.

The model is conceptually shown as a 'bow-tie' model (see section 2.4.4) however in practice this part of the BN is not created by using the fault tree top event as the event tree initiating event, as this conceptual model might imply. Instead, a new variable is created with a state for each of the 14 possible outcomes. In the new variable each of the outcome states is true only if that outcome is true in the event tree part of the model and a derailment has occurred (i.e. the top event variable of the 'fault tree' part of the model is true). The NPT for this new variable is therefore simply an AND truth table. However it is not necessary to complete this table in the Hugin BN model, as an equivalent logical statement can be used instead.

The output node multiplies the probability of occurrence of a derailment with the probability of occurrence of each outcome calculated by the BN event tree, given that a derailment has occurred.

Models of this type combine calculations of the probability of occurrence of some event with a scaling factor relating to exposure data i.e. the number of times that there is an opportunity for this event to occur. For example, the derailment model within the SRM calculates the risk from derailments across the network as a whole in a given year, based on historical incident data. It then divides this figure by the total number of train miles on the network per year to give an approximation of the risk from derailment per train mile. This is based on the principle that, although a derailment event occurs in a specific place the opportunities for derailment rise as the number of train miles rises.

The model developed here applies the same principles but in a slightly different way. It has been structured to calculate the probability of occurrence of a derailment on a given section of track in a given year. To scale the output an average train demand of approximately 200 trains per day (73,000 trains per year) is assumed. This assumption, and the normalisation of train traverse events that it enforces, is appropriate given the intended uses of this prototype model; the relative comparison of the risk at different types of track location (see section 8.12).

For different studies, for example to explore the impact of timetable changes on derailment risk on a particular section of track, it would be necessary to scale the output for different demand rates, measured in train miles. This could be done simply by dividing the output probabilities of the model by 73,000 and scaling them up by the desired demand rate.[8] To develop the model to more readily support scaling in this way this could be done by dividing the probabilities of occurrence of the relevant prior probabilities in the model (a subset of the fault tree base events) by the assumed demand rate. The revised model would then output a probability of occurrence per train mile in the same way as the SRM.

8.8 Data requirements and model quantification

As discussed in section 2.1.1, the probability estimates that form the likelihood component of risk can be estimated using a combination of historical data and expert judgement. This approach was followed to quantify the derailment BN model described in this chapter.

Several data sources, which provided probability estimates similar to those needed to quantify many of the BN NPTS, were identified and reviewed. The data sources were:

---

[8] The SRM does not provide any facility to vary exposure data automatically and any scaling of risk to take account of exposure is similarly done outside of the model.

- The core derailment study, which formed the basis of the event tree BN described in the previous chapter
- Probability estimates developed with the author of the core derailment study, as part of the BN event tree modelling approach described in the previous chapter
- Probability estimates provided in the Risk Solutions Report (Campbell and Kennedy 2003).

In all cases the available data needed to be supplemented by a significant degree of judgement. In addition to this, in many cases in the model there was no data at all to inform the elicitation of conditional probability estimates. Therefore an elicitation process was undertaken, supported by two of the risk analysts from Sotera who developed the network wide risk model for Irish Rail (see section 5.2). These analysts supported a probability elicitation process in two separate meetings. The NPTs for the model were populated using the same process as is described for the event tree model in section 7.3.3. Where data relating to the frequency of occurrence existed, or where others had sought to estimate similar probabilities and the relevant conditions were known, this data was used to populate the NPT. Where data was absent, NPT tables were completed via extrapolation and judgement using available data as reference values. The full set of NPTs for the model, and the sources of data used are described in Appendix C8.

8.9 Types of condition modelled

In section 2.3.1.3, conditions were categorised as being of four types: technical, operational, organizational and performance. These categories are used to differentiate between the different types of condition modelled in Table 12. Note that three different types of condition are modelled.

Technical	Operational	Performance
containment fitted track curvature number of tracks track type lineside object density lineside object type location of track	competence of infrastructure maintenance worker competence of rolling stock maintainer driver experience	track inspection intervals rolling stock inspection interval line speed

Table 12: Types of condition included in the parameterised BN model

The model has been developed for use to estimate derailment outcome frequency rates in any location on a particular section of the UK rail network where conditions states are known. Therefore, in order to derive meaningful outcome frequency estimates every condition must be set to a particular state in the BN before the BN probabilities are updated. The model does not include any prior distributions across the states of condition nodes and so the output of the model is meaningless if any condition nodes are not set. It may be possible to extend the model so that it could calculate risk estimates across a particular section of the network, or set of locations, but to do so would require an understanding of the distribution of conditions across that set of locations and the correlations between the conditions. This approach is investigated further in section 10.3.2.

The ease with which the state of conditions can be established in any particular circumstance is related to the type of condition, according to the previous categorisation of causes.

'Technical' conditions are the fixed physical attributes of the railway infrastructure. There is no conceptual barrier to the identification of 'Technical' condition states. Their state should be able to be determined in any particular location by inspection. Even if these condition states were not contained in asset registers they would be able to be identified by an inspection.

The state of operational conditions tends to be more difficult to ascertain than the state of a technical condition. In the model, the competence of individuals is stated as an operational condition. This could be established via audit but implies a different level of scrutiny for 'operational' conditions compared to 'technical' conditions. There may also be some subjectively in assigning 'operational' condition states, such as assigning 'high', 'medium' or 'low' levels of competence.

Performance conditions are set parameters of the network and can be planned and changed according to management decisions. These conditions might change rapidly from minute to minute or might suddenly change after a period of months or years. The states of these conditions can be estimated, using the railway's planning information but ultimately the states will be subject to perturbation and change.

The set of conditions selected for the model reflects those identified by the expert judgement process previously described. In the UK rail industry, we are concerned with fundamentally the same accidents and hazards. Therefore, were these models to be built we would expect that the set of relevant conditions would rapidly emerge through

the shared experience and understanding of the industry just as the set of 125 hazardous events modelled by the SRM has emerged.

Note that no 'organizational' conditions were identified as part of this process. The issue of 'organizational' conditions will be revisited in section 10.3.

8.10 Testing the model output

In this section, a number of tests of the model are described. These were undertaken to:

- ensure that the model was free from unintentional errors
- establish whether the model produced estimates that were similar to those calculated from a trusted industry model (the SRM).

8.10.1 Implementation of fault tree logic in the BN model

Tests were undertaken to confirm that the fault tree logic had been correctly encoded in the BN. Different sets of evidence were entered into the condition states in the BN, so that fixed base event probabilities could be established. Fault trees were then built to calculate the top event probability using these fixed base event probabilities. In all cases identical top event probabilities were calculated by the BN and by its fault tree equivalent (see Appendix C.9.3).

8.10.2 Derailment occurrence rates

The output results were then compared with derailment rates calculated by the SRM. This was done in order to investigate whether the fault tree output of the BN model was comparable to other probability estimates in the rail industry which were known to be trusted. The condition states shown in Table 13 were identified as a set of conditions that might exist in a typical location on the UK railway network. These conditions were then entered into the BN model so that it calculated the derailment risk in a 'typical' location and the evidence propagated through the net to update the calculations.

As discussed in section 8.5, evidence is not entered into nodes representing failure type and severity to undertake calculation of accident probabilities. These nodes relate to events not conditions. Instead, as can be seen from the NPTs for these variables, they are instead quantified with prior distributions. These distributions were estimated by averaging over the different fault types based on knowing their relative rate of occurrence across the UK rail network. These variables are therefore not shown in Table 13.

In the fault tree part of the model, there are five gates that input to the top event (Gate 2 – over speed derailment occurs, Gate 3 – track fault derailment occurs, Gate 13 – S&C (Switch and Crossing) derailment occurs, Gate 17 – rolling stock fault derailment and Gate 21 – obstruction derailment). Each calculates the probability of occurrence of a different type of derailment. These probabilities were taken from the BN model and compared with their equivalent values from the SRM. The two sets of probabilities are shown in Table 14.

Conditions	Typical mile section of UK rail network
containment fitted	No
track curvature	low/none
line speed	40-79
number of tracks	2
track inspection intervals	2 week
track type	switch and crossing
lineside onject density	Low
lineside object type	Anchored
location of track	outside rural
rolling stock inspection interval	2 weeks
competence of infrastructure maintainer	Medium
competence of rolling stock maintainer	Medium
driver experience	Medium

Table 13: Conditions for a typical location on the UK rail network

	Probability per track mile per year, calculated using BN model with the condition states shown in Table 13 set.	Probability per track mile per year, calculated by aggregating relevant SRM precursor rates (see Appendix C9.4)
Gate 2 – over speed derailment occurs	4.50e-10	8.11E-10
Gate 3 – track fault derailment occurs	1.16e-08	1.41E-08
Gate 13 – S&C (Switch and Crossing) derailment occurs	4.60e-09	9.69E-09
Gate 17 – rolling stock fault derailment	1.12e-09	1.47E-09
Gate 21 – obstruction derailment	9.19e-08	3.17E-08

Table 14: Derailment probabilities calculated by the BN and by the SRM

The probabilities of occurrence for gates 2, 3, 13, 17 and 21 are all of the same order of magnitude as their SRM equivalents. This finding can be explained. As discussed in

section 4.2, the SRM model output does not relate to any particular mile of track on the network. It is simply the number of hazards occurring in total, divided by the number of train miles in total. The SRM figure therefore represents the network average likelihood of occurrence of a derailment. Analysis shows that this estimate is similar to the estimate the prototype model produces for a typical section of the network.

8.11 Use of the model

In the absence of a full set of data the BN model has been developed with a limited data set, supported by judgement. Therefore the model cannot be considered to be a fully validated risk model suitable for use in real risk management problems.

Nevertheless the model structure and probabilities have been based on the judgements of industry risk analysis experts, and quantified using available data. The test described in 8.10.2, provides additional confidence that the model output is credible. The model combines a large number of causal relationships and in isolation each relationship is plausible. The combined effect of these causal relationships on the probability of occurrence of derailment accidents has never previously been modelled in this way. Therefore despite lack of substantial data to quantify the model I believe the output of this model may still provide meaningful support to the previous hypotheses. The philosophy is similar to that of Ale et al (Ale, Bellamy et al. 2006) who argue that an educated guess, based on a carefully designed and constructed model is better than unsupported judgement alone.

Section 3.6.3 argued that risk is highly variable from location to location, resulting in the occurrence of 'hotspots'. I now investigate whether the model does indeed show such variation.

The model is used to see what level of risk it estimates for locations with characteristics similar to those where the Hatfield and Potters Bar derailments occurred. All of the evidence entered into the BN models is information that could be routinely obtained or monitored at locations across the network in advance of the occurrence of an accident. However not all of this information is currently gathered in a suitable form. The condition 'competence of infrastructure maintainer' refers to the organisational competence, and it is considered that a qualitative judgement of this organisational attribute could be ascertained by regular audit of the application of an organisation's competence management system. These sorts of audits are a requirement of railway companies' safety management systems, and are therefore undertaken regularly in the GB railway industry. Although there is no standard approach that is universally applied

across all companies each company would apply some sort of qualitative assessment of management processes and this could be linked to the qualitative categories assigned in the model (high, medium and low).

8.11.1 Hatfield Scenario

Table 15 shows two sets of conditions entered into the prototype BN model. The first set represents the conditions existing in a typical mile section of high speed track on the UK railway network. The other represents a set of conditions similar to those that existed at the location of the Hatfield derailment in 2000.

Conditions	Typical section of high speed track	Hatfield type scenario
containment fitted	false	false
track curvature	low/none	high
line speed	110-125	110-125
number of tracks	2	4
track inspection intervals	2 week	4 week
track type	plain line	plain line
lineside object density	low	high
lineside object type	anchored	anchored
location of track	outside rural	outside rural
rolling stock inspection interval	2 weeks	2 weeks
competence of infrastructure maintainence	medium	low
competence of rolling stock maintainer	medium	medium
driver experience	medium	medium

Table 15: Conditions set for a typical track and a Hatfield type location

Each set of conditions were entered into the BN model in turn and the output probabilities calculated.

Scenario		Typical location (prob per track mile per year)	Hatfield type location (prob per track mile per year)	scale of difference
1	No derailment	0	0	0
2	Minor derailment within clearances	4.01E-07	2.81E-07	0.7
3	Major derailment to cess, tunnel portal hit	0	0	0
4	Minor derailment to cess	2.53E-07	9.72E-07	3.8
5	Minor derailment to cess, striking lineside structure	6.50E-08	2.50E-07	3.8
6	Minor derailment to cess, collapsing rolling stock	4.33E-08	1.67E-07	3.8
7	Major derailment to cess	9.38E-07	3.61E-06	3.8
8	Major derailment to cess, striking lineside structure	3.03E-07	1.17E-06	3.8
9	Major derailment to cess, collapsing rolling stock	2.02E-07	7.78E-07	3.8
10	Major derailment to adjacent line, tunnel portal hit	0	0	0
11	Minor derailment to adjacent line	3.61E-08	8.33E-07	23
12	Minor derailment to adjacent line, with secondary collision	3.25E-07	3.33E-06	10
13	Major derailment to adjacent line	1.44E-07	3.33E-06	23
14	Major derailment to adjacent line, with secondary collision	1.30E-06	1.33E-05	10
TOTAL		4.01E-06	2.81E-05	7

Table 16: Tabulated model output for a typical location and Hatfield type

Table 16 shows the derailment outcome probabilities calculated for each location. The column on the right hand side shows the difference between the values calculated in each location as a ratio. Figure 42 presents these results visually, using a logarithmic scale for the occurrence probability.

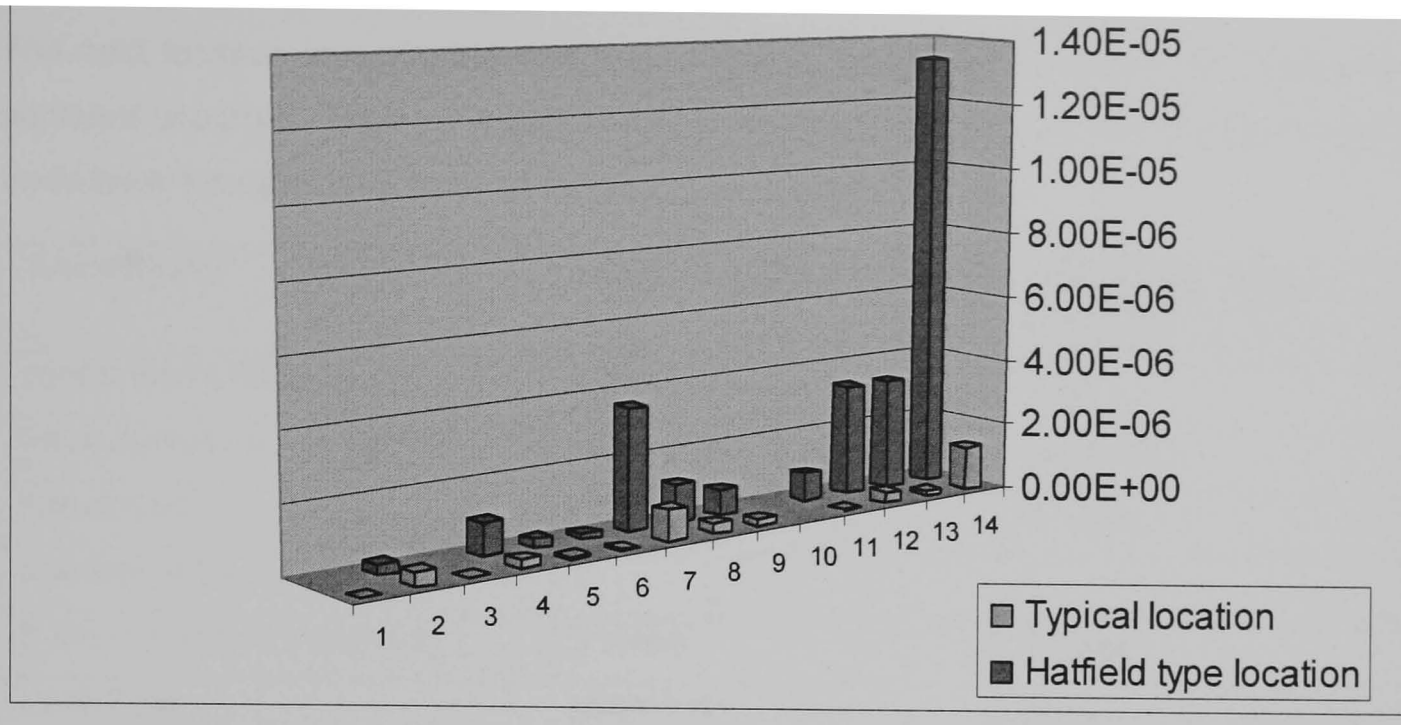


Figure 42: Graph of model output for a typical location and Hatfield type

Table 16 shows that the probability of occurrence of a derailment of any type is 7 times more likely in the Hatfield type location than in the 'typical' high speed location selected. The graph shows that the probabilities of occurrence of all possible accident scenarios in the Hatfield type location are significantly higher than those in the 'typical' location with the exception of outcome 2 'minor derailment within clearances' (which is a low severity outcome relative to the other outcomes).

The train in the accident at Hatfield collided with the overhead catenary and ruptured the restaurant coach, where all of the fatalities occurred. This scenario relates to Accident 9: 'Major derailment to cess, collapsing rolling stock'. The model calculates that this particular accident outcome is approximately 4 times more likely in a location with conditions similar to the Hatfield accident, than in a 'typical' high speed location. The model calculates a much higher probability of major train accidents to the adjacent line, including a much higher probability of secondary collisions (outcomes 11 to 14). Although this did not occur at Hatfield, it is clear that such accidents were very possible, and could well have occurred in different circumstances. .

Risk is the product of accident likelihood and severity. The differential calculated and shown in Figure 42 is in the probability of accident outcomes only. The model does not calculate the severity of accidents. If this were done, then the differences in the speed associated with the two scenarios would be likely to result in an even larger factor of difference between the risk estimates in each location than that shown for the accident outcome probabilities.

8.11.2 Potters Bar scenario

The next location investigated was one similar to the location in which the Potters Bar accident occurred. Table 17shows two sets of conditions entered into the BN model to undertake the calculations for comparative purposes.

Conditions	Typical section of track	Potters Bar type scenario
containment fitted	false	false
track curvature	low/none	low/none
line speed	80-109	80-109
number of tracks	2	4
track inspection intervals	2 week	2 week
track type	plain line	S&C
lineside object density	low	high
lineside object type	anchored	fixed
location of track	outside urban	outside urban
rolling stock inspection interval	2 weeks	2 weeks
competence of infrastructure maintainer	medium	low
competence of rolling stock maintainer	medium	medium
driver experience	medium	medium

Table 17: Conditions set for a typical track and a Potters Bar type location

Table 18 shows the derailment outcome probabilities calculated for each location. As with the previous example, the column on the right-hand side shows the difference between the values calculated in each location as a ratio. The results are presented in Figure 43 .

Scenario		Typical location	Potters Bar type location	scale of difference
1	No derailment	0	0	0
2	Minor derailment within clearances	1.33E-07	1.81E-07	1.4
3	Major derailment to cess, tunnel portal hit	0	0	0
4	Minor derailment to cess	3.00E-08	1.70E-08	0.6
5	Minor derailment to cess, striking lineside structure	2.50E-09	2.27E-09	0.9
6	Minor derailment to cess, collapsing rolling stock	8.33E-10	3.40E-09	4.1
7	Major derailment to cess	2.83E-08	1.59E-08	0.6
8	Major derailment to cess, striking lineside structure	3.75E-09	2.72E-09	0.7
9	Major derailment to cess, collapsing rolling stock	1.25E-09	4.08E-09	3.3
10	Major derailment to adjacent line, tunnel portal hit	0	0	0
11	Minor derailment to adjacent line	3.33E-09	1.36E-08	4.1
12	Minor derailment to adjacent line, with secondary collision	3.00E-08	5.44E-08	1.8
13	Major derailment to adjacent line	3.33E-09	1.36E-08	4.1
14	Major derailment to adjacent line, with secondary collision	3.00E-08	5.44E-08	1.8
TOTAL		2.66E-07	3.62E-07	1.4

Table 18: Tabulated model output for a typical location and for Potters Bar type

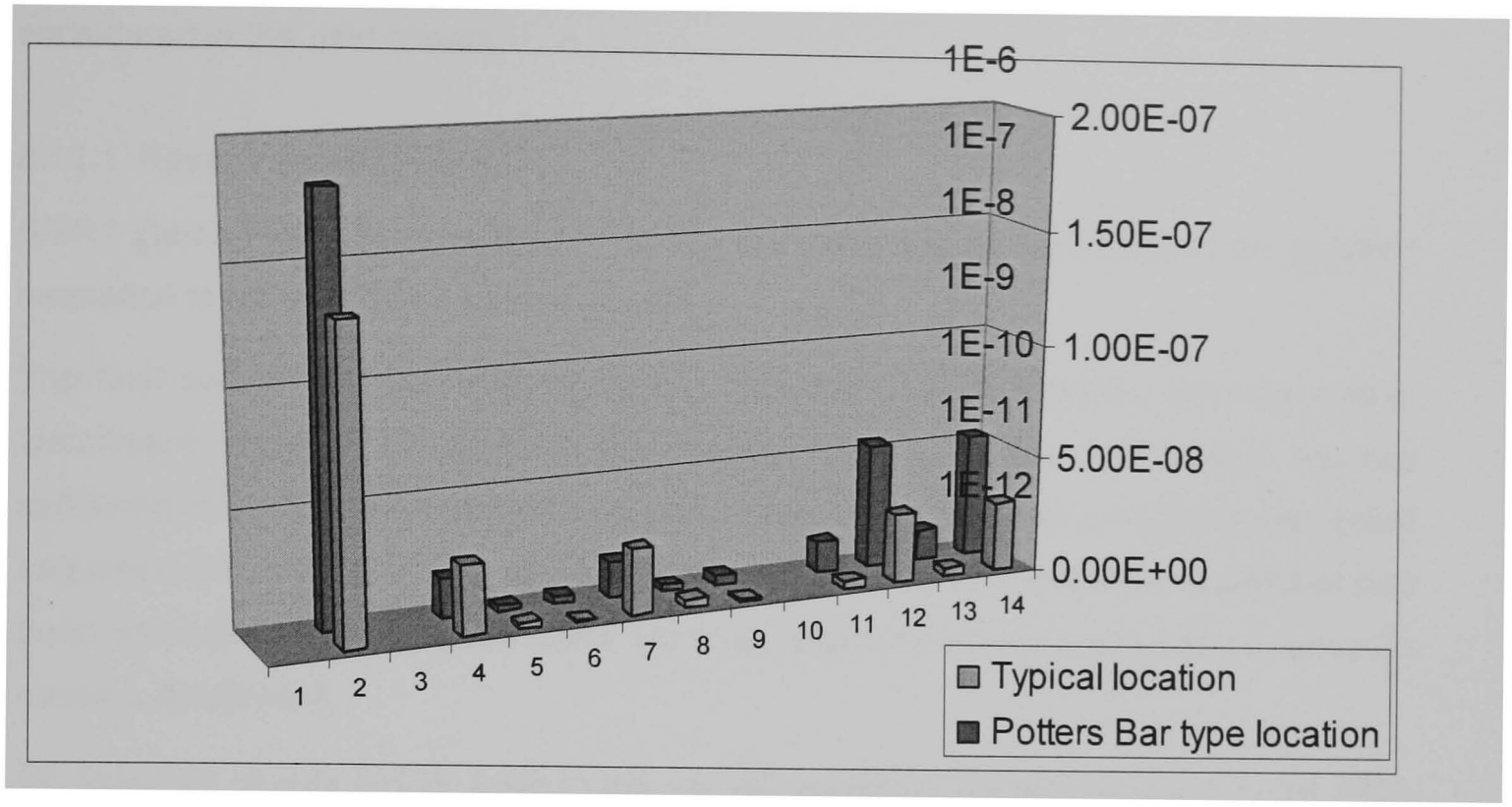


Figure 43: Graph of model output for a typical location and Potters Bar type

From Table 18 it can be seen that that the total probability of occurrence of a derailment is only very slightly greater in the Potters Bar type location than in a 'typical' location. However, the difference is less pronounced than it was in the previous example. This might be thought to indicate that the Potters Bar derailment was in some way less foreseeable than the Hatfield accident. Ultimately this might be because the model includes more of the causal factors that were relevant to the Hatfield accident than were relevant to the accident at Potters Bar. The Potters Bar accident was fundamentally caused by a points maintenance error. The analysis does not assume any knowledge about this failure, and without this specific knowledge there is little information that does indicate this location as being particularly prone to a derailment.

This analysis does indicate that, were a derailment to occur in a location where the set condition states existed, the derailment would be likely to have severe consequences. The train is assumed to be travelling very fast and its proximity to lineside structures creates the potential for severe collisions.

8.12 Review of the prototype model and its potential benefits

In this section, I argue that parameterised risk models of the type described in this chapter meets the ideal requirements for risk modelling RMR1-RMR3 that were proposed in section 3.8. On this basis, I partially argue hypothesis 4, that the development of risk models that meet the ideal characteristics set out is possible. The

degree to which the model meets remaining two requirements (SMS1 and SDM1) is considered in the next chapter.

8.12.1 Review against RMR1

RMR1 states that: 'Risk models should allow for as many of the events in an accident sequence to be modelled as is practicable.'

The fault tree part of the SRM modelling derailment cause includes only one event: 'derailment occurs'. This event is then categorised by its possible causes. As was explained in section 8.1 the fault tree part of the model includes a much longer event sequence than the SRM. The deepest model of cause in the derailment model that has been produced relates to track faults. Up to six separate events might need to occur to cause a derailment.

By definition events further back in the causal sequence will tend to occur more often than those later in that sequence. The BN model therefore identifies events that are likely to occur often enough to make monitoring of their occurrence possible and provides a structure with which to analyse and interpret that data.

8.12.2 Review against RMR2

RMR2 states that: 'Risk models should allow all significant and quantifiable technical, operational, organizational and performance conditions that cause accidents or exacerbate risk to be explicitly modelled.'

The BN model makes significant progress in this area. The model demonstrates how a wide range of conceptually different conditions can be explicitly included in the model. The model includes conditions from three of the four categories of condition that were initially identified: technical, operational and performance. However, the inclusion of organisational conditions has not yet been demonstrated (the inclusion of such factors is addressed in section 10.3.1). Inclusion of such factors is needed before the approach could be argued to be entirely consistent with organisational accident theory. In the review of the industry risk assessment (appendix A and section 4.3), it was established that analysts do take account of technical and operational condition states when determining the likelihood of events in the accident sequence. Despite this, they do not always document this process rigorously. The approach outlined in this chapter is based on exactly the same sort of judgements. More of them are required which would create development and analysis work initially. However, the condition states would then be thoroughly documented. As the description of the relationships between

events and conditions in the model is general, the model could be used repeatedly and possibly shared between organisations who manage risk on the railway. This means that a particular model would evolve and improve over time, and there would be no need to continually develop risk models for different applications from first principles.

Operational conditions like 'competence of infrastructure maintainer' are also commonly used to inform the estimation of event likelihoods. For example these conditions are typical of those that form the 'error producing conditions' in some human factors assessments (see section 2.3.1.2). The condition 'competence of infrastructure maintainer' refers to the organisational competence, and it is considered that a qualitative judgement of this organisational attribute could be ascertained by regular audit of the application of an organisation's competence management system.

8.12.3 Review against RMR3

RMR3 states that: 'Risk models should be parameterised by conditions so that the risk at different locations and in different situations on the railway network can be rapidly recalculated.'

The prototype BN derailment risk model is parameterised by 13 different conditions. These each have between two and five possible states. In theory, the model is capable of calculating derailment accident probabilities for over 620,000 different sets of conditions. This is not to say that that many different combinations of condition states actually exist in locations on the UK railway network. Rather that, in practice, the model has sufficient resolution to differentiate between all possible combinations of those condition states.

In models reviewed previously, different condition states were incorporated by physically duplicating parts of the fault and event trees. This approach was applied in both the SRM (see section 4.2) and in the model produced by Risk Solutions (see section 5). In the latter case the approach resulted in a model of unmanageably large size. A greater degree of parameterisation than that attempted in that research project has been achieved by applying a modular approach. The fault and event tree branching structure is used as the modular core of the BN. Setting condition states in the BN automatically restructures the fault and event tree models encoded in the BN for the purposes of calculation.

The derailment model was used to test the theory that risk occurs in 'hotspots' across the network, where the conditions that give rise to organizational accidents exist. Conditions for locations similar to those known to have existed prior to the derailment

accidents at Hatfield and Potters Bar were entered into the model, and the output compared with that calculated in 'typical' locations where 'typical' condition states existed. The model calculated much higher probabilities of occurrence of all types of derailment accident in both cases. In particular much higher probabilities of occurrence were calculated for the accident outcomes which most closely matched those that actually occurred in each case. Therefore in both cases the output of the model supports organizational accident theory and the idea that given readily available or collectable data, and the right model to interpret it, risk hotspots can be identified prior to the occurrence of major accidents.

8.13 Review conclusion

The arguments put forward in sections 8.12.1 to 8.12.3 show that the models of the type described in this chapter meet three of the five requirements for ideal risk models that were proposed in section 3.8. The requirements were developed to specify a risk model with organisational accident theory as its conceptual basis. The approach does not currently demonstrate how organisational conditions could be explicitly included and therefore does not provide a complete realisation of a model aligned to this theory. However the use of BNs as the base of the model provides opportunities for further work to expand the model in the area of organisational conditions, which are discussed in section 10.3.1. The degree to which the model meets the remaining two requirements (SMS1 and SDM1) is considered in the next chapter.

8.14 Chapter Summary

In this chapter, I described a risk model, developed using a BN, and based on fault and event tree logical structures. The model is parameterised by making condition states explicit and variable and is quantified using available data and expert judgement.

The model is flexible enough to be used for rapidly analysing risk in different locations. By entering sets of conditions similar to those in which major accidents are known to occur, it was demonstrated that the model would have identified these locations as having much higher probabilities of major railway accidents occurring than a typical railway location. In the case of the Hatfield accident the model estimates the risk from the particular accident that occurred as being several orders of magnitude higher than at a typical location.

I argued that parameterised risk models, of the type described in this chapter, meet the ideal requirements for risk modelling RMR1-RMR3 that were proposed in section 3.8. On this basis I have partially argued hypothesis 4, that the development of risk models

that meet the ideal characteristics set out is possible. I argue that the modelling approach meets remaining two requirements (SMS1 and SDM1) in the next chapter.

9 Using a parameterised risk model to support safety management and decision making

In Chapter 8 a parameterised BN risk model was described and its uses investigated. It was argued that this model substantially met the modelling requirements (RMR1-RMR3) that were previously outlined.

In this chapter, the argument in support of Hypothesis 4 is completed by arguing that the parameterised risk model meets the remaining two ideal requirements that were initially set out in this thesis, namely that it:

- Effectively supports the various stages of a safety management system (SMS1).
- Is capable of being used and understood by those who manage safety on the network (SDM1).

In order to argue that the model meets these requirements, I outline how such a model would be developed (see section 9.1) and used in practice (see sections 9.2 and 9.3).

9.1 Methodology for the development of a BN risk model

This section describes the process by which a BN risk model of the type described in Chapter 8 would be developed. Although, as has been demonstrated, it is feasible to build such models using off the shelf BN software packages, this is very time consuming. Additional tool support would be necessary to ease the development of these types of model for practical application. The description of the development methodology is supplemented with views that could be produced using software, which would support the process used to develop these types of model.

The software envisaged to support the development of the model would need to support the following functions

- Fault tree editing
- Event tree editing
- BN editing and inference calculation

The software envisaged would have similar editing functionality to existing commercial editors like Fault Tree plus (Isograph 2007) for the fault and event tree modelling. BN editing and calculation would require similar functionality to software like Agena risk (Agena 2008) or Hugin (Hugin 2008). The fault tree user interface would be viewed using standard fault tree notation of the type described in section 2.4.2 and shown in

Figure 38. The event tree software user interface would display event tree notation of the type described in 2.4.3. The BN user interface would similarly display a BN notation as described in Chapter 6.

In addition to model viewing, editing and calculation functions the software would allow the causal model to be viewed either as a fault and event tree or as a BN. Alternative views would be generated by automating the translation process described in sections 6.4.4.1, 7.3.1 and 7.4.1.

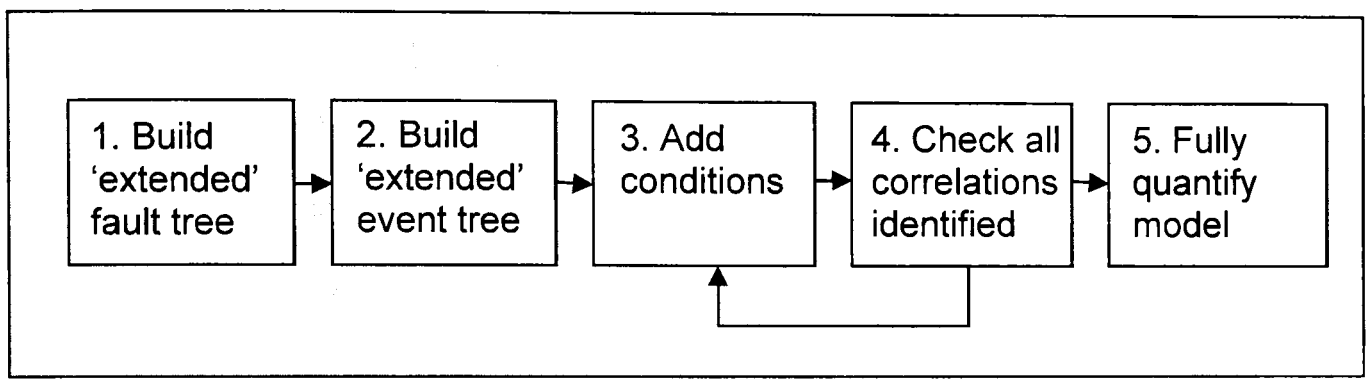


Figure 44: Methodology for the development of a parameterised BN risk model

Figure 44 shows the five stages in the development process. Each of these stages is described in the following sections.

9.1.1 Stage 1: Build 'extended' fault tree

First, the model architect develops the 'extended' fault tree using a fault tree editor. The extended fault tree would be developed following standard approaches to fault tree modelling, by reviewing the hazard and seeking to identify the set of technical faults or human errors that, individually or in combination, could lead to its occurrence. Note that each BN model models the risk from a particular hazard. For example, the model described in Chapter 8 considers only a derailment hazard. In order to model all risk to which the railway network is exposed, the process would have to be followed for each separate hazard that might arise on the network.

Ideally, the model architect should develop the fault tree model to as low a level of abstraction as is practicable in accordance with requirement RMR1. Control measures that might be applied to reduce risk tend to align with events in the model. Therefore a greater depth of causal analysis means that the model can ultimately be used to investigate the possible impact of a wider range of control measures. Fault Tree models commonly model sub-system failures, and in some case go down to several levels of abstraction modelling component level failures. A greater depth of analysis leads inevitably to a larger number of base events that must be quantified. Ultimately the decision about the depth of causal analysis will be taken based on weighing up of

the benefits of inclusion of additional base events, against the costs. There are two main benefits of including more fault tree base events:

1. The model will be able to be used to investigate the implications of a wider range of failures on risk.

2. The model, when parameterised, will be able to be scoped to represent a wider range of different locations and situations, allowing more explicit modelling of the failure mechanisms for locations in which these additional failures might occur.

These benefits must be weighted up against the cost of the time and effort needed to collect and analyse the additional data that would be required to quantify any additional fault tree base events. Also, there are some events that there is little practical experience or understanding of and it is not possible to judge credible event probabilities for such events. Figure 45 shows a simple example of what the extended fault tree might look like for the purposes of illustrating subsequent stages of the development methodology.

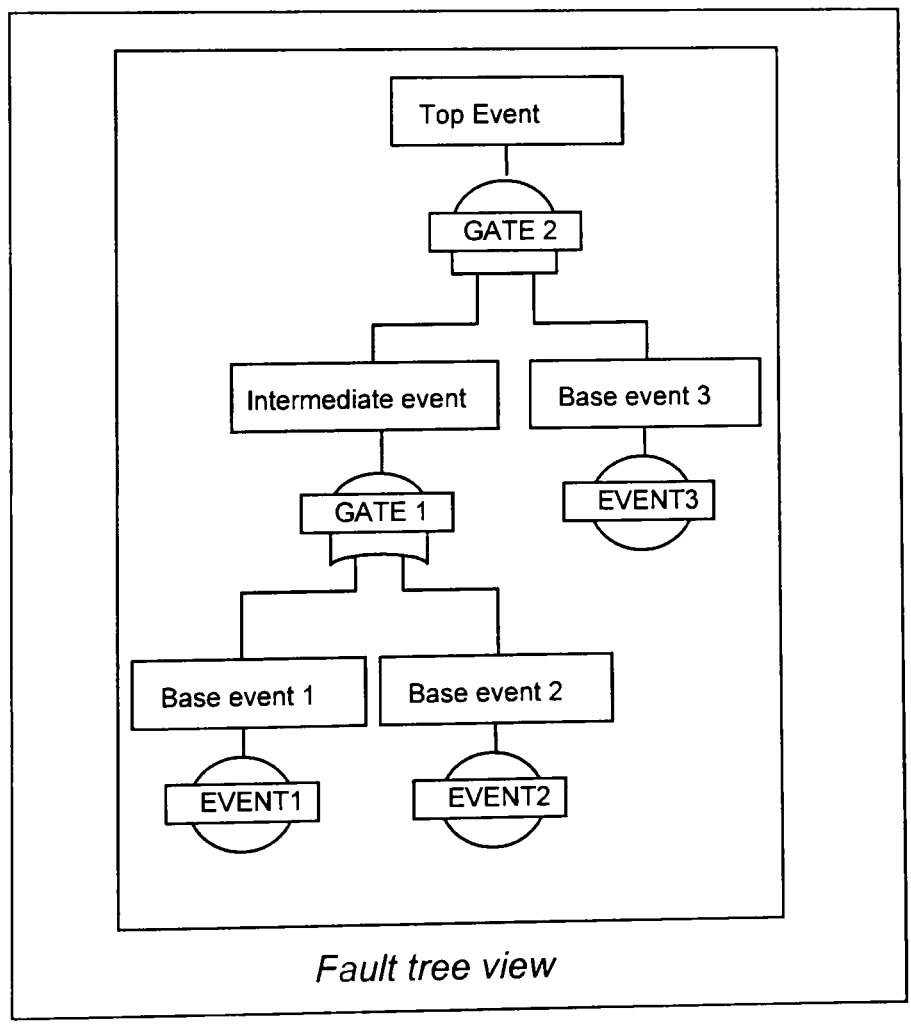


Figure 45: Simple example of an extended fault tree

At this stage, the extended fault tree does not include any base event probabilities, as it represents only the generic logical structure of events whose occurrence can lead to

the occurrence of the hazard under analysis. It is the railway network equivalent of the Major Logic Diagrams or 'top logic' used for modelling failures in nuclear industry systems (see section 5.4, page 100).

The 'extended fault tree' developed for the top event 'train derailment' (Appendix C.4.1) gives an indication of the size and complexity of fault tree that is envisaged for this approach.

9.1.2 Stage 2: Build 'extended' event tree

Next, the model architect develops an 'extended' event tree using an event tree editor. The extended event tree includes all possible event sequences following the occurrence of the hazard. A simple illustrative example is shown in Figure 46. Note that no probabilities are shown on the model at this stage. The model shows the full set of possible events and the range of possible combinations of those events leading to discrete outcomes. The event branching logic defined clarifies where certain event combinations are either impossible or irrelevant to outcome consequences in all circumstances (i.e. under all possible combinations of condition states). For example, the diagram shows that, given that event 4 is false, the probabilities of occurrence of event 5 and event 6 are irrelevant to the outcome, regardless of the states of any conditions that might subsequently be considered.

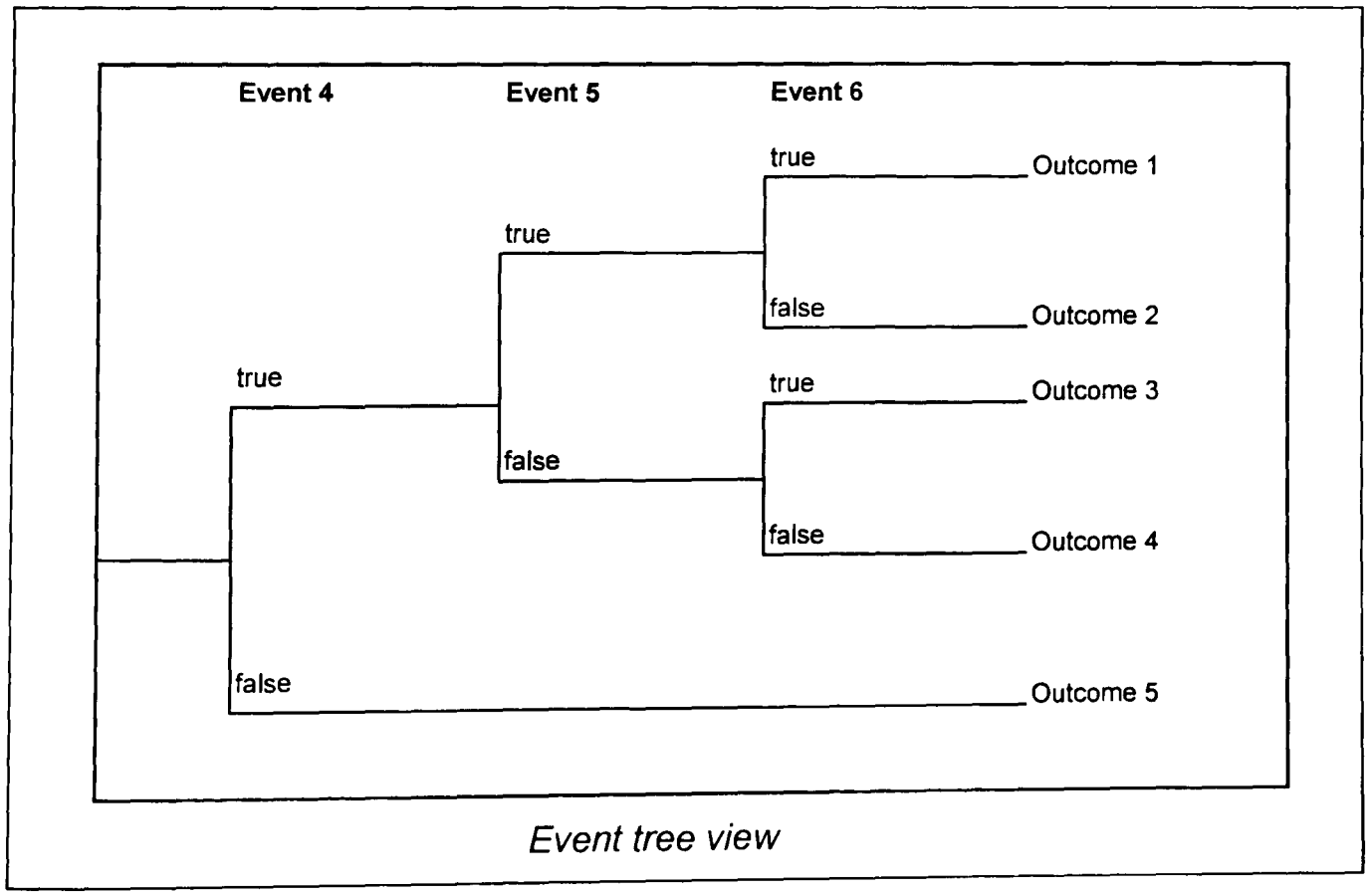


Figure 46: indicative extended event tree

The model architect could develop an entirely new event tree using expert knowledge and available data. However, as with the modelling undertaken as part of this thesis in Chapter 8, sets of existing event trees might be used to help build the tree. The analyst must make a judgement as to how many events to include in the model. Like the fault tree part of the model, the event tree part models events in possible accident sequences. The same trade-off of the benefits of including additional events against the costs, as described in 9.1.1 is required. For a risk model for the UK railway industry it would be sensible to use, or at least refer to, the sets of event tree models produced as part of the SRM. These models have been developed over many years to represent the industry's understanding of the possible sequences of events that can occur on the UK railway network as a result of hazards and therefore provide an indication of the level of detail which should be possible.

9.1.3 Stage 3: Add conditions

Conditions would be added to the model in the BN view of the 'extended' fault and event trees. The model architect would identify the conditions whose state can affect the probability of occurrence of each event and add these into the BN. A checklist type approach could be used to derive the list of conditions. In this thesis four different types of condition that might be modelled have been categorised. The model described in Chapter 8 demonstrated how conditions of three of these types could be modelled. The checklist approach could be structured around these categorisations and might include the following prompts:

- Technical conditions (e.g. types of train, attributes of the surrounding location)
- Operational conditions (e.g. frequency of planned inspections, competency of individuals)
- Performance conditions (e.g. speed, track inspection intervals)

Ultimately, the relevant conditions are determined by the type of system or network being modelled. Both parts of the case study described in this thesis, demonstrated how industry risk analysts and experts could derive the relevant set of conditions for a particular analysis. Setting the states of technical conditions is simple. For example, there are known, defined, types of trains and data relating to their population across the railway network could be obtained. However for other types of condition definition of variables and associated variable states is more difficult. Some states are qualitative and judgement based. For example in case study 2 some competency variables (see for example Figure 41) were assigned the qualitative states 'high', 'medium' and 'low'.

Definition of these states, and assigning of them to real world conditions is subjective. However, the definitions could be linked to the results of audits, for example audits of the competence of members of the workforce, as was the case with the aviation BN modelling project described in section 6.4.3.1. Assigning a value of 'medium', for example, would be considered to be a qualitative assessment based on performance relative to norms of current practice or behaviour in a particular area. Although the assignments are subjective, it is reasonable to believe that some correlation between, for example, audit results and the actual competence of individuals and departments would exist. If the inclusion of such factors in the model were found to be useful and beneficial then this would imply the need to improve the consistency and repeatability of audits of this type, in order to improve the use of these types of variables to support modelling and safety management.

For a set of accidents in a particular industry, the relevant conditions would be expected to emerge over a period of time as they are intrinsic to the type of system being operated, and the nature of possible accidents. However, as with modelling decisions about the number of events to model, there is a cost-benefit judgement to be made about how many conditions and condition states to include. The more that are included, the wider the range of potential uses of the model, and the more likely that the model's assumptions could be aligned to a particular scenario by instantiating evidence into the BN. However inclusion of additional conditions and their states greatly increases the size of the BN NPTs, and therefore greatly increases the effort required to quantify them. This is potentially even more problematic than quantification of event probabilities as, as was discussed in section 3.6.2, complete data sets relating to conditions states on the GB rail network are not readily available. The inclusion of conditions states should therefore be prioritised to those whose states are known to most strongly influence one or more of the events in the accident sequence. For existing fault and event tree type models these conditions will tend to be the things stated as the key assumptions of the model.

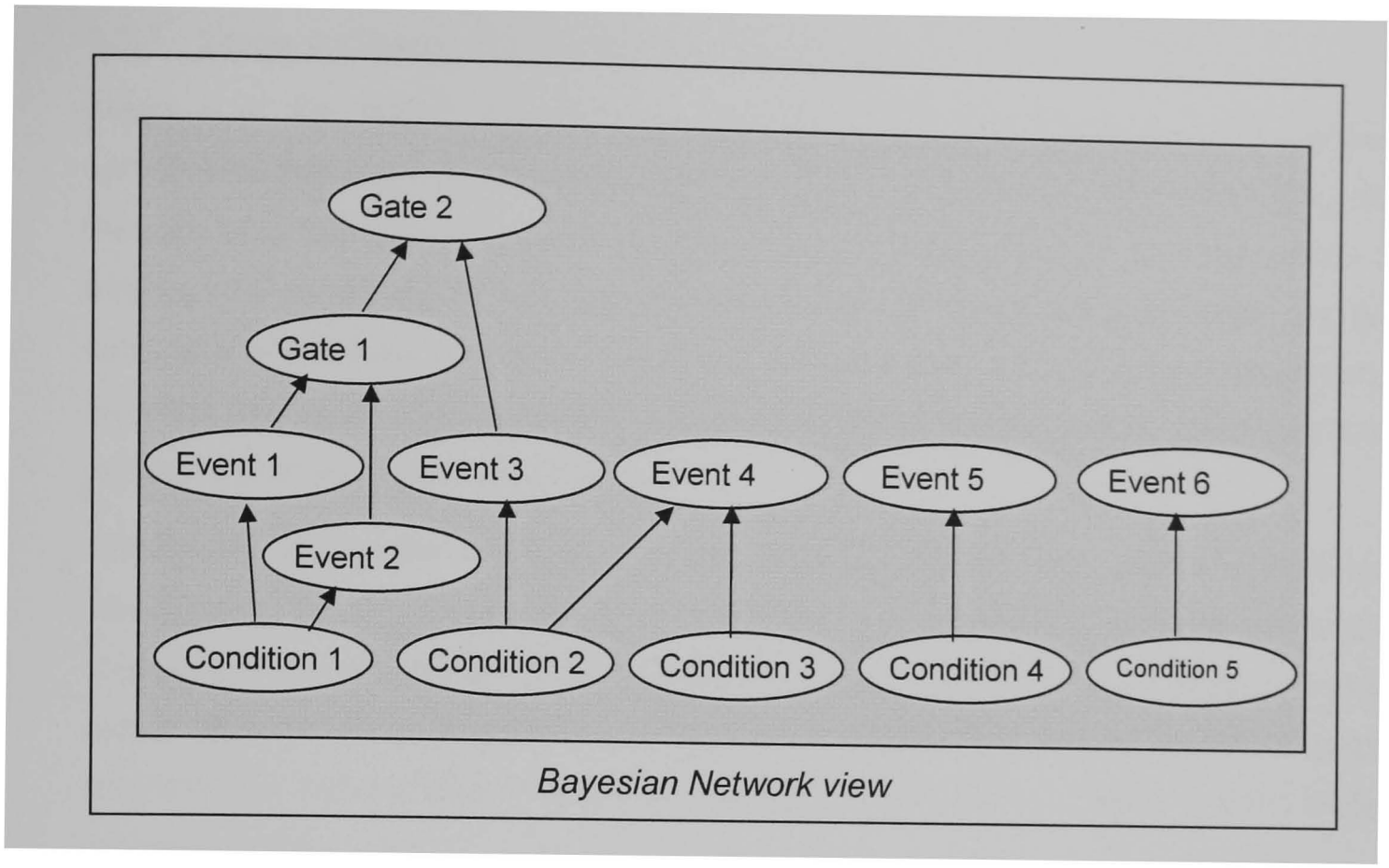


Figure 47: BN view of conditions and events

Once conditions have been identified the model architect inputs the causal relationships between conditions and events by adding causal arcs between them. The diagram of Figure 47 shows the BN view of the extended fault and event trees with the addition of five condition nodes whose states are considered to influence the probability of occurrence of one or more events.

The fault tree of Figure 45 has been translated into its BN equivalent by applying the translation process described in section 6.4.4, and the event tree section of the BN at this stage in the process shows only the set of events included in the extended event tree. This view does not show the nodes used to calculate the event outcome probabilities as they do not provide any additional information or understanding that is considered helpful. In the example shown each event is affected by one or more conditions and each of these conditions has two possible states. Note that condition 2 influences event 3, which is in the fault tree, and event 4, which is in the event tree. This shows how the model is able to overcome the assumed independence of a fault and event tree in a simple bow-tie model that was discussed in section 3.4.4, in a clear, transparent way. The model does not require the input of prior probabilities on all condition nodes. This is because, when the model is used, there are a set of condition nodes whose state must be certain for meaningful risk estimates to be calculated by the model (Table 11 shows the list of the conditions for which prior probabilities were required in the derailment model).

9.1.4 Stage 4: Check all correlations identified

Stage 4 of the model development process is a check to ensure all necessary correlations between variables have been included as arcs in the BN model. To do this the use of a correlation chart is proposed. A correlation chart is a simple matrix of events and conditions which indicates where causal relationships between the two exist, and where they do not. Completion of the chart ensures that causal relationships between events and conditions have been considered systematically. Table 19 shows an example of such a correlation chart.

Correlation charts are a simple way of ensuring that the risk analyst consciously considers all potential correlations in the model, and consciously rules out any where correlations are not shown. Missing these correlations would have an effect on model output calculations and would also result in an imperfect graphical model of causal relationships. Full correlation charts for the model described in Chapter 7 are included in appendix C6.

	line speed	rolling stock inspection interval	competence of rolling stock maintainer	rolling stock fault type	rolling stock fault severity
event 17- rolling stock fault occurs	No	No	No	**Yes**	**Yes**
event 18 – derailment occurs (rolling stock fault)	**Yes**	No	No	**Yes**	**Yes**
event 19 – rolling stock fault detected	No	**Yes**	**Yes**	**Yes**	**Yes**
event 20 – rolling stock fault not fixed	No	No	**Yes**	No	No
event 21 – train stays in service	No	No	**Yes**	No	No

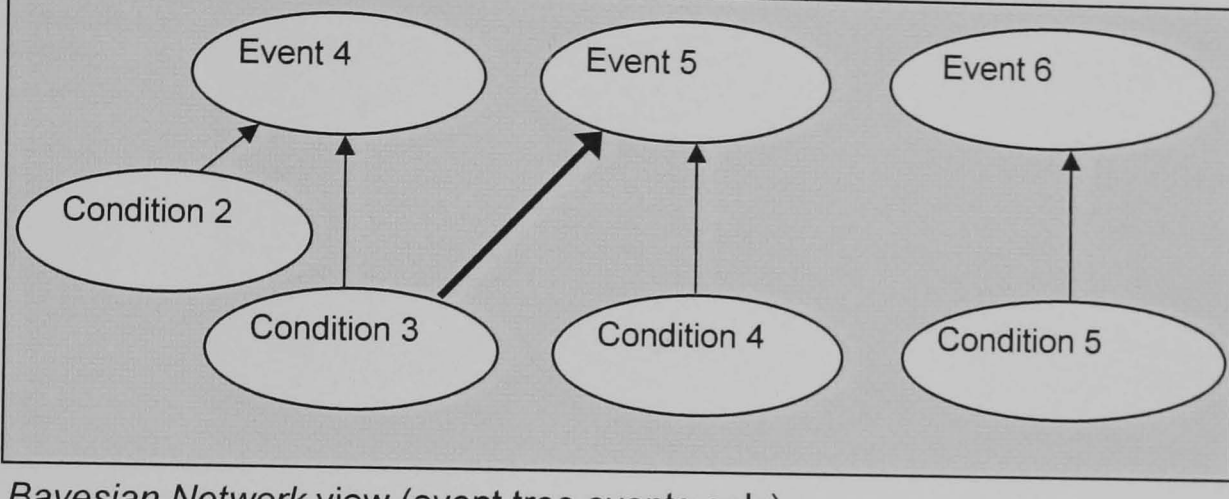
Table 19: Example correlation chart

The software should support the use of correlation charts of the type shown in Table 19. It should generate a table of the set of events (both event tree events and fault tree base events) in the model and highlight where these have been correlated to conditions by the inclusion of directed arcs. The software should allow the editor to assert the existence of conditional probability relationships in the chart. The software would need to ensure that, when these additional correlations are added to the chart, the BN representation of the model is automatically updated to ensure that the equivalent arc is also added.

Additional causal arcs should be automatically inserted into the BN representation when correlations are identified in the correlation chart view. Figure 48 shows the identification of an additional causal arc between condition 3 and event 5.

	Event 4	Event 5	Event 6
Condition 2	Yes	No	No
Condition 3	Yes	**Yes**	No
Condition 4	No	Yes	No
Condition 5	No	No	Yes

Correlation chart generator/editor view



Bayesian Network view (event tree events only)

Figure 48: Adding correlations into the chart creates additional BN arcs

9.1.5 Stage 5: Quantify model

Next, the model is quantified by entering the probabilities of occurrence of faults and events. There are several stages to the NPT quantification process. The model architect must undertake the following tasks:

- Enter sets of condition states relevant to a particular location or situation
- Enter the relevant fault and event probabilities into the fault and event tree views of the model.
- Repeat for a number of cases (locations or situations)
- Complete the NPTs by extrapolation using available data and expert judgement.

All four stages are together described in the following text.

First, a set of conditions that represent a particular situation or location are entered into the model. Once condition states have been entered, the model architect should be able to view the resulting fault tree or event tree. The view produced would show the extended trees annotated with the relevant condition states. Figure 49 shows the

extended event tree annotated to show condition states and example probabilities entered on the basis of these condition states.

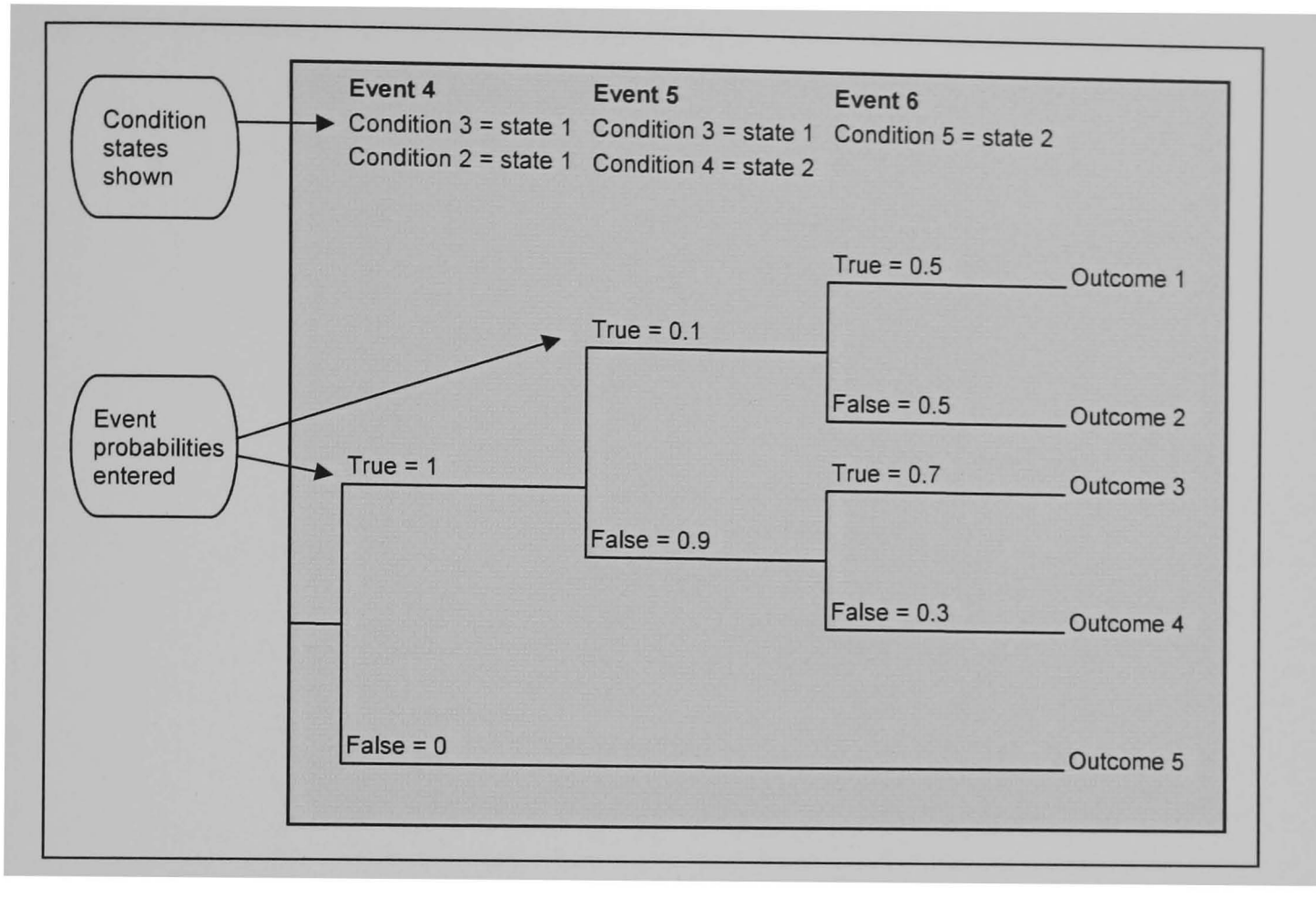


Figure 49: Event tree view annotated to show condition states

Given this view of the event tree, the model architect can input the probabilities of occurrence of each event into the model with complete knowledge of the states of the relevant conditions. In other words, the diagram is annotated to make all key assumptions clear and hence much of the ambiguity associated with unclear or average assumptions (for example the issues discussed in section 4.3.2) are removed.

Figure 49 shows that the model architect has entered different probabilities for event 6 depending on whether or not event 5 is true. This indicates a conditional probability relationship between event 5 and event 6. This conditional dependency could be identified automatically and captured as an arc when the complementary BN model is subsequently produced (see Figure 51).

The model architect would input a range of sets of condition states indicating different locations or situations. For example, in the industry study that was reviewed previously 6 different sets of conditions were identified (section 4.3). The model architect would need to be confident that enough different cases had been considered to uncover the full set of events relating to the hazard under analysis and all conditional probability relationships between events.

Figure 50 shows a similarly annotated version of the extended fault tree. Again, this view shows the condition states which influence base event probabilities. The diagram also shows example probabilities entered on the basis of these condition states.

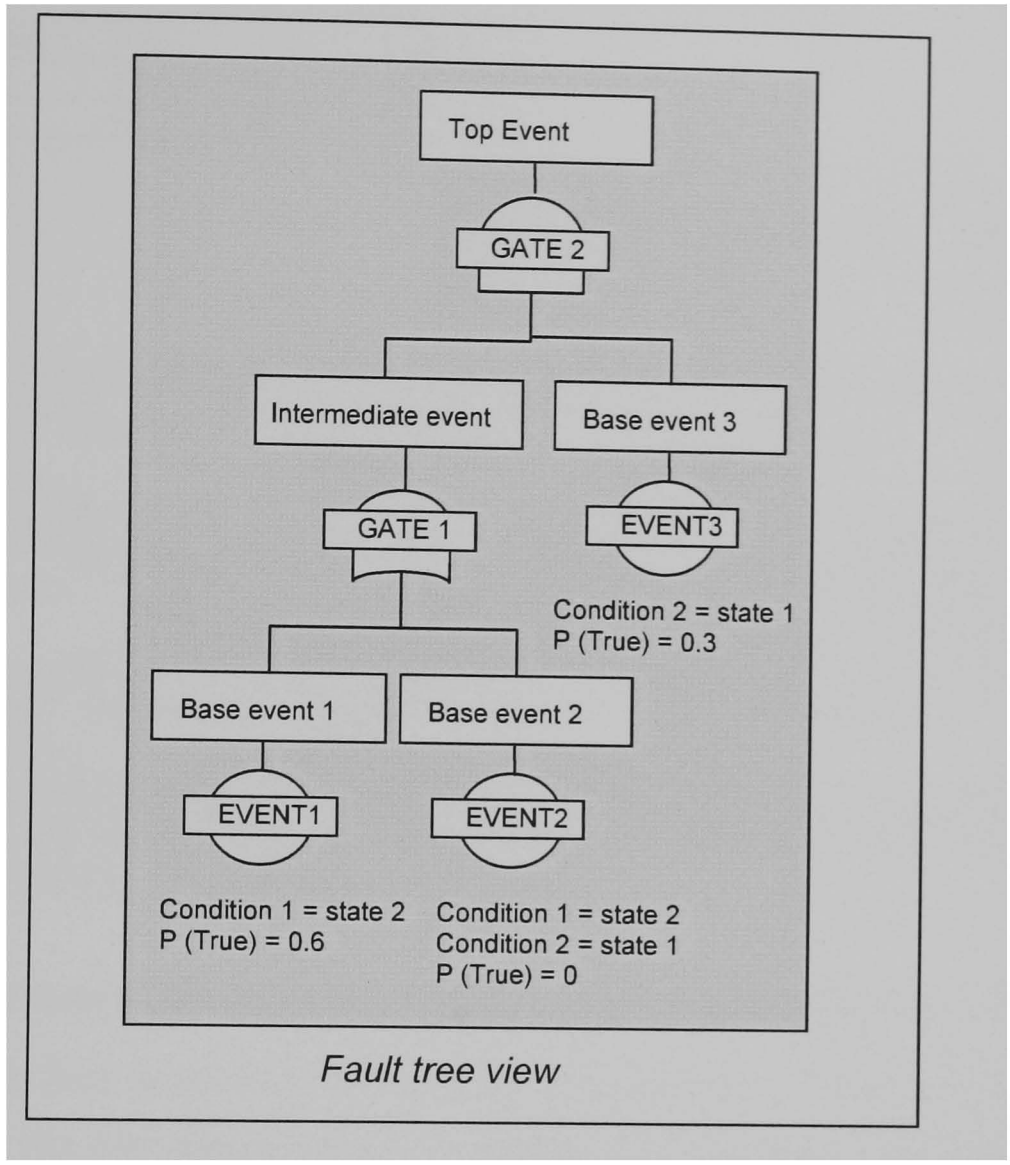


Figure 50: Fault tree view annotated to show condition states

The final stage in the quantification of the model is to complete the full set of fault and event probabilities needed by the model. To do this the model architect would revert to a BN view of the model produced to support NPT quantification. The BN view of the event tree event nodes and associated conditions is shown in Figure 51. Note also that the BN view produced captures the conditional probability relationship between event 5 and event 6 that is indicated by the probabilities assigned in Figure 49.

In this view of the model, the model architect would be able to see where event probabilities had been entered and where they remain unquantified. The diagram shows that there is at least one probability of occurrence in each event NPT shown. The model architect therefore has a reference value to use to extrapolate the remaining probabilities in the NPT. In other words the analyst estimates the likely causal influence relationship between two variables based on an understanding of the relationship

between the two values. The existing values in the NPT provide point estimates which the conditional probability relationship described in the NPT must fit.

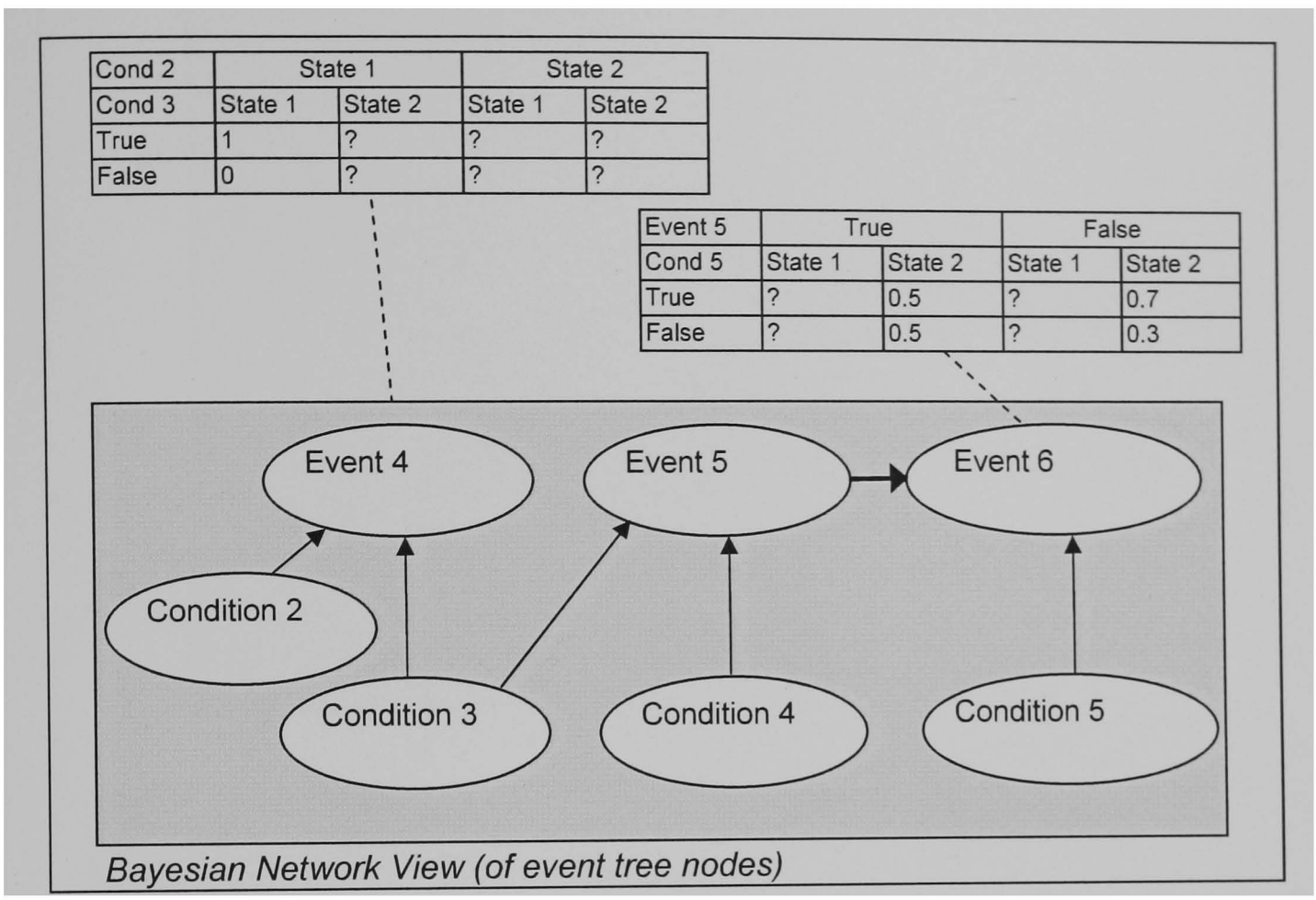


Figure 51: BN view of the event tree nodes model with partially populated NPTs

The model architect does not need to view the event tree model to undertake this judgement as the BN clearly shows all influences of interest. This approach was applied to the quantification of the BN derailment model described in this thesis (section 7.3.4 and 0).

Quantification of the fault tree model would follow a similar process. Figure 52 shows the BN view of the extended fault tree model and related conditions, with the NPTs populated according to the base event probability assignments shown in Figure 50. In practice, the model architect would need to populate the model with probabilities based on sufficient different sets of circumstances to ensure that at least one set of probabilities was included in each NPT. The model would be able to be used when all event node NPTs are complete.

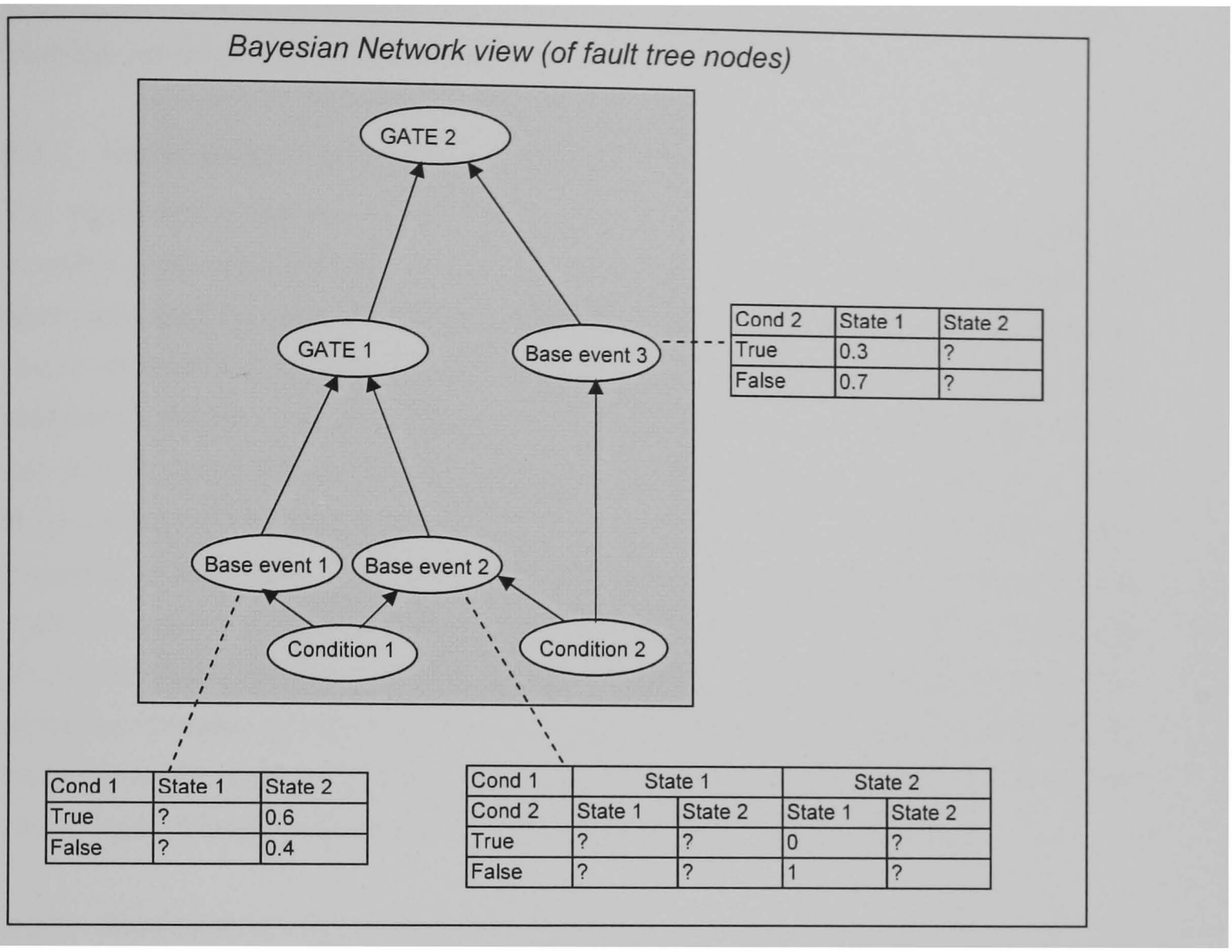


Figure 52: BN view of the fault tree nodes with partially populated NPTs

9.2 Using the model to support safety management

Having explained how the BN modelling approach would be developed in practice, I next explain how it would be used to support safety management activity. The extent to which the model could be used to support the various elements of a Safety Management System, as initially proposed in section 3.7.2 is considered. This is to allow subsequent consideration of the extent to which the modelling approach meets requirements SMS1.

Note that the model described in Chapter 8 does not yet calculate risk, and the methodology described in this chapter does not describe how this would be done in practice. The model described calculates the probability of occurrence of undesirable accident outcomes. In order to use the model to calculate risk, it would first be necessary to assign a severity to each accident outcome. Then it would be necessary to calculate and aggregate the risk associated with each branch of the event tree part of the model by multiplying the likelihood and severity of each branch outcome (implementing Equation 1). This section describes the use of the model to assess and

analyse risk given that this approach presents no theoretical barriers and is therefore possible, although it is not described how it would be done in detail.

9.2.1 Use to gauge the impact of organizational changes on risk.

The derailment model described in Chapter 8 only includes three of the four types of condition that were defined in section 2.3.2. I have not yet demonstrated how the approach could be used to model organizational conditions. However, in the literature review of section 6.4.3 several areas of research were identified where others have proposed a variety of approaches for the incorporation of organizational conditions into risk models using BNs. The work described in this thesis has demonstrated how to build a robust BN for the UK railway industry that builds on and extends existing safety engineering techniques. There is therefore an opportunity to extend the modelling approach such that the BN could include organizational conditions, either by adopting proposals made by others or developing a new approach which capitalises on the apparent suitability of BNs to this type of modelling problem. This is investigated as possible future work in section 10.3.1. Therefore the model does not meet this requirement but it provides the potential for future development in this area.

9.2.2 Estimates the total network wide risk

The model is potentially capable of calculating the aggregate risk across the entire network. This could be achieved by:

- Developing a BN model for each of the hazards that are possible on the network.
- Estimating the risk associated with each possible instance of the hazard across the network so that the total risk could be aggregated to estimate the total network rate.

This would require that the condition states in a large number of locations and situations were separately determined and entered into the model for each estimate to be calculated. This process could be automated by automatically reading sets of condition data relating to each network location into the model, and summing the results. A safety manager could use such a model to estimate the locations with the highest probable accident rates so that safety management effort could be prioritised to address them. (Marsh and Bearfield 2007b) uses a train SPAD example to demonstrate how this could be done with the use of a 'situation node' to set the

combinations of condition states for each location in the correct proportions for an infrastructure area.

However, the approach would only be possible if all condition information in each location was known and for the reasons that were outlined in section 3.6 this is not currently the case. However the model provides a clear specification for data that, if known, could be used to estimate accident occurrence rates. This issue is considered further in section 9.2.5.

In summary, the model is potentially capable of being used to estimate the network wide accident outcome frequency rates. The modelling approach provides a specification for the collection of the data necessary to model the aggregate railway safety risk across the UK network. If this data were collected and systematically fed into the model it would allow network wide risk totals to be calculated.

In section 10.3.2 an approach for estimating network wide risk totals in the absence of such data is discussed as a possible extension to the work described here.

9.2.3 Estimation of risk by individual location

Because the model is parameterised, it allows the user to closely align model assumptions with knowledge of the condition states that exist in particular locations and at particular times on the network. Using the BN model, it is a simple matter to recalculate accident probabilities given each different set of condition states, and by applying this approach it is possible to identify risk hotspots on the railway network. This use is equivalent to the analysis that was demonstrated in section 8.11.

The analyst would enter all necessary condition states relating to a particular location on the railway network which was suspected of having a disproportionately high accident risk associated with it – i.e. of being a risk hotspot. A risk estimate for this particular location or scenario could then be calculated. To determine whether risk is relatively high comparison could be made with 'typical' locations, as was done in the analysis described in section 8.11. Separate fault and event tree models would be produced in each instance meaning that analysts would have a qualitative model of the underlying accident event sequence in addition to numerical estimates of risk.

Using this type of risk model, it is possible to differentiate between a large number of different sets of conditions. The model developed in Chapter 8 is theoretically capable of estimating the risk in over 620,000 different sets of circumstances. The approach therefore removes the need to make average assumptions. In the core derailment study model the analyst assumed that track curvature was severe, even though he

knew that in some cases track curvature was moderate and in other locations track was straight. Therefore even if data is not available to support quantification of the model, the fact that the model provides greater context and clarity of key assumptions should make the basis of elicitation much clearer, and hence improve the ease of elicitation, and creates the potential for more accurate risk estimation of probabilities.

In summary, the model clearly supports estimation of risk by individual location, as this underpins the requirements that it was designed to meet (in particular RMR3).

9.2.4 Estimate changes in risk levels following interventions

Once a high risk level has been identified, by either of the means described in 9.2.3 or 9.2.2 a safety manager would then need to decide what to do to manage or reduce that risk.

As described in section 2.1.3, the railway industry bases decisions about whether or not to introduce new control measures for safety reasons on a comparison of the risk reduction achieved by a measure and its costs. The model provides a means of determining the risk reduction associated with a control measure, in order to support this process.

The model results in the development of standard fault and event tree views of the accident sequence, and it is possible to view underlying BN fragments which describe additional causal relationships. The analyst could use the model to postulate the possible effect of various interventions. The rich causal models produced, and the use of existing safety engineering models, would help an analyst or editor to understand the fundamental causal sequence, and therefore aid them in identifying where the imposition of control measures might be most effective.

An accident occurs due to an undesired sequence of events. Each event in the accident sequence provides an opportunity for intervention and prevention and hence risk reduction. Control measures are therefore targeted at the prevention of certain events in the accident sequence or at the conditions which influence the probability of occurrence of those events. For example by reference to Figure 40, derailment risk would be decreased by putting in place a detection measure, like a rolling stock fault inspection. This is modelled as an event 'rolling stock fault detected'. However given that such a detection measure is in place derailment risk could be further reduced by improving the competence of the track inspector, or by increasing the regularity of inspections. These two causes relate to conditions – 'competence of infrastructure maintainer' and 'rolling stock inspection interval' respectively. Where control measures

targeted the state of conditions the risk reduction they might achieve could quickly be estimated by entering different condition states, associated with the before and after scenarios and calculating the difference in risk.

In some cases, where a control measure fundamentally changes the nature of the event sequence, and causal relationships, it might be necessary to undertake bespoke fault and event tree analysis to estimate the risk following the imposition of this control measure. Even in this situation the parameterised model could provide help by providing a clear baseline model, in which all key assumptions are clearly documented.

As the models are at a deeper level of cause than the other models reviewed in this thesis, it would provide the potential for a wide range of control measure to be considered using the model.

In some cases there may only be a few locations where intervention is necessary. Using a highly parameterised model or the type developed by following the methodology described here, it should be possible to differentiate between a wide number of locations on the network. This means that the model can be used to help target control measures to the set of locations where they would be most effective.

An analysis that was scoped to look at infrastructure areas rather than individual locations, like the SRM or the core derailment study, might fail to identify these interventions. In other cases network wide models might justify the imposition of control measures in general, but fail to identify the subset of locations where installation is not necessary. I previously described how the industry implemented TPWS at junction signals across the entire railway network in order to reduce SPAD accident risk. Some of these installations were subsequently removed as they were considered to cause operational problems without having any significant affect on risk. Using a model of the type described here it would have been possible to estimate the risk reduction achieved by TPWS in each different location or type of location. Control measures could then have been targeted at the locations where they provided the best reduction in risk. This would have resulted in more efficient allocation of the railway's resources.

In conclusion, the modelling approach strongly supports the estimation of changes in estimated accident rates following interventions.

9.2.5 Monitoring risk

The problems with the monitoring of data for the purposes of supporting risk assessment in the UK railway industry were summarised in section 3.6:

- Because the industry operates with high levels of safety there is little readily available accident data with which to ascertain the effectiveness of defences against accidents, at any given point in time.
- Major accidents are often the result of a complex set of causes that are particular to a location or situation. Data relating to the variety of causes that might be implicated in a major accident is not routinely monitored.
- The sheer size and variability of the railway network means that the amount of potentially relevant data is vast. This makes collection and interpretation of data very difficult.

The model provides improvements in each of these three areas, respectively by:

- Providing a richer causal model that goes further back in the event sequence and hence identifies events and incidents which occur more regularly and hence can be monitored
- Explicitly models a wide range of accident causes, both events and conditions, making it clear what causal information should be recorded following an accident or incident, to support risk estimation
- Identifying the causal data that can usefully be collected, and hence being used to identify data that might be collected for other reasons. The model could also be used to identify the data that could be collected as a priority. The model provides a means of interpreting the data collected and using it to calculate risk. This allows for risk itself to be estimated and monitored and also provides a justification for detailed incident cause reporting.

The model shows the variables (both events and conditions) whose state is related to the probability of occurrence of an accident. Data is needed to improve the understanding of these relationships in order to quantify the conditional probability relationships that are essential to the model. Data on the occurrence of events and the states of conditions allows estimation of event occurrence rates and how they differ given the presence of certain sets of conditions. The modelling approach described in this thesis supports monitoring as it can be used to improve a company's awareness of what event and condition data should be monitored to ensure the best possible estimate of risk. A risk model produced following the methodology developed lists the

events in the event sequence and all of the conditions whose state is known to influence the probability of occurrence of these events. The model could therefore be thought of as a specification of the data that should be recorded by an organisation to support the estimation of risk. As the model includes a long causal sequence, with a wide range of conditions modelled as influencing these events, the result is a very detailed and thorough specification of the data that should be routinely collected in order to support risk modelling in the industry.

The risk model identifies events that are further back in the causal chain. These events will by definition occur more often than hazards and accidents creating more opportunity for monitoring. The availability of this data should therefore make it more easy to elicit likelihood estimates and logically would give greater confidence in the accuracy of overall estimates. Accurate estimates of the likelihood of these events will improve the ability to estimate the likelihood of subsequent events, and ultimately of hazards and accidents. The model therefore identifies the events whose rates of occurrence can be monitored to improve understanding of risk.

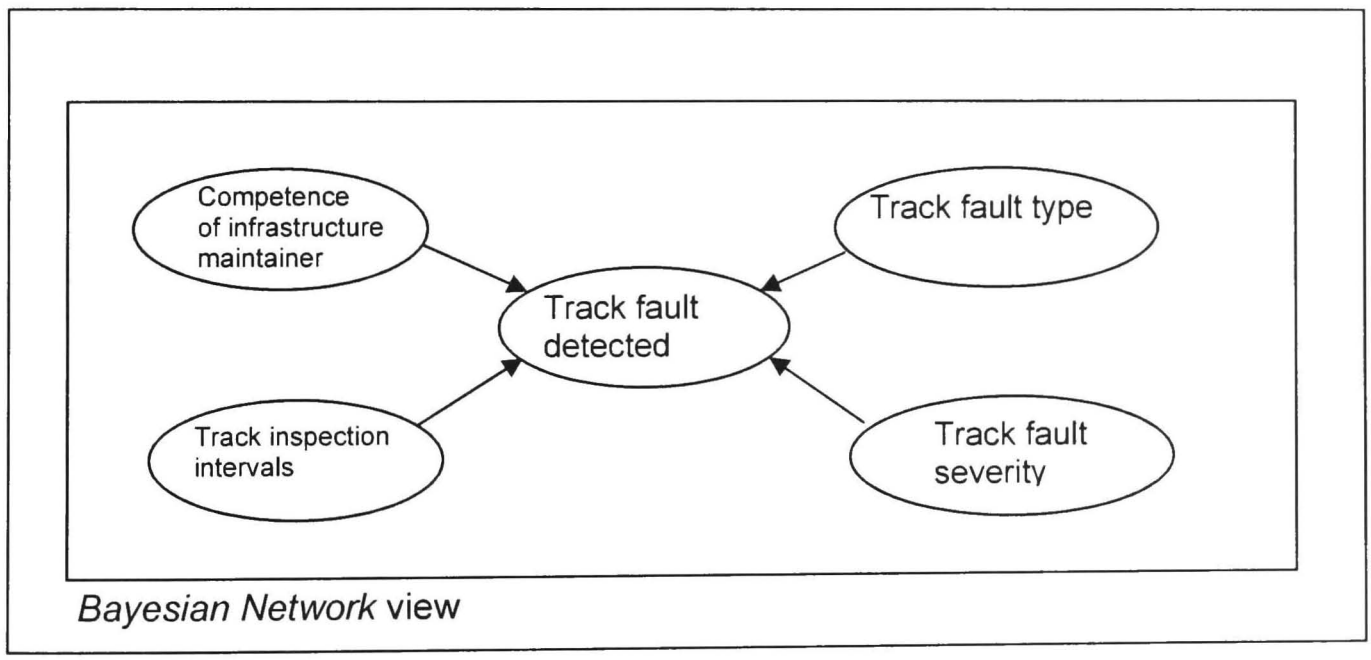


Figure 53: BN model fragment: nodes influencing whether a track fault is detected

Figure 53 shows the set of conditions whose state influences the event 'track fault occurs'. These are 'competence of infrastructure maintainer', 'track inspection intervals', 'track fault type' and 'track fault severity'. The implication of this is that data relating to the states of these conditions should be routinely collected, and in particular should be recorded when a track fault occurs.

Knowledge of the state of conditions when events have previously occurred would help the industry to build up a map of all condition states across the network and at different

time of the day or year. It would also help determine the strength of correlations between events and conditions. The condition states represent the circumstances in which an event occurs. If the likelihood of occurrence for an event in a certain set of circumstances can be established then this is likely to provide a good likelihood estimate when those same circumstances arise again. However, this data is not necessarily relevant where the circumstances differ. Collecting condition data is therefore a way of avoiding the 'loss of context' problem (section 3.6.2). If condition data is routinely collected when an event occurs, data becomes more useful in the future as its relevance to other similar situations can be established.

The BN model developed has a significantly larger scope and higher resolution of causal analysis than traditional event trees or sets of event trees. This means that to quantify the model many more probability estimates are needed. This remains a key barrier to the adoption of the modelling approach. As was discussed in section 0, however, some types of condition data are more readily available than others. Technical conditions should be able to be established via asset records or via survey. Performance conditions may change rapidly from minute to minute or might suddenly change after a period of months or years however they are at least constrained to an extent by readily available plans such as the timetable. These conditions therefore provide the obvious starting point for establishing better knowledge of condition states and using them to drive risk models.

Operational and organizational conditions may be more difficult to ascertain requiring proactive measures for their identification and qualitative judgements about their particular state. I have not demonstrated how organizational conditions like safety culture indicators could be included in the model, although this remains an aspiration and is discussed in the subsequent chapter.

If the correct information is recorded, relevance of data to event probabilities given different conditions can be properly established when quantifying the model. The model supports the use of this data in the elicitation of probabilities as elicitation would ultimately come down to a succession of judgements about the degree of correlation between two variables. It also supports the sharing of data between organisations. Data collected by one organisation at one location on the network, might be useful to another organisation at another location on the network, where the same or similar conditions exist. A BN model shared across operators on an infrastructure area, with relevant conditions agreed between them, would make it possible to pool incident data and allow organisations to learn from others' data. The model allows the set of conditions to be established when using data to support probability estimation, and also

when using the model to estimate risk in a particular location. The flexibility and structure of the model allows the user to re-establish that context when using the model for analysis. The model therefore creates the structure for the industry to jointly learn from data that is collected.

In summary, the model provides a specification for the data that should be collected in order to estimate risk. The amount of potentially useful data is significant and therefore collecting it would be time-consuming. This is a barrier to the adoption of the approach. However the model supports better elicitation of probabilities and identifies data items that could be readily collected in the immediate future.

9.2.6 Can be used to help learn lessons from accidents

Application of the methodology produces fault and event tree models of the generic event sequences in addition to the BN causal model. This provides a detailed qualitative model that could be used by those investigating the occurrence of an accident to help understand the sequence of events that may have occurred, and the possible condition states that existed at the time of the accident.

Any accident that occurs due to a particular hazard should fit within the generic risk model associated with that hazard. If this is not the case, then it implies that the model is incomplete and needs to be updated.

9.2.7 Can be used to diagnose the causes of accidents

BNs are commonly used to diagnose the causes of events (see section 6.4.1). However reasoning from effect to cause is not possible using BN models of the type described in this thesis. In section 10.3.3, it is explained why this is the case and further work that might overcome this limitation is suggested.

9.2.8 Ability to be used to interpret audit results, and their implications for risk

According to the definitions of conditions that were proposed in section 2.3.2 organizational conditions could be considered to be 'failings or inefficiencies in an organisation'. Operational conditions could be considered to be 'factors that affect the performance of front line staff undertaking safety related duties'. Either of these conditions might be audited. The model described includes some operational conditions in the model and hence indicates how audit results might be used to inform the estimation of risk. As previously stated, the model that was presented in Chapter 8 does not include organizational conditions and I do not claim to have demonstrated that it is possible to include such conditions in the model. However, the BN modelling

approach developed means that it may be possible to extend the approach in this area, and future work to investigate this is proposed (see section 10.3.1).

9.2.9 Summary of review against SMS1

The model substantially supports the application of a safety management system in the areas of:

- estimation of risk by individual location (section 9.2.3) and in
- estimation of changes in risk levels following interventions (section 9.2.4)
- monitoring of the railway to support risk estimation and modelling (section 9.2.5)

In the other areas reviewed, the model either partially supports safety management or provides or provides promising areas of further work where it could be developed to do so more fully.

In general, the model supports the various elements of a safety management system more fully than the other approaches reviewed (in Chapter 4) and provides a foundation for further development in this area. Therefore it partially meets SMS1, and provides the foundation for development to meet this requirement more fully as I will go on to investigate in sections 10.3.1 to 10.3.3.

9.3 Use of the model to support safety decision making

Having described how a model would be developed and the views that a tool would need to show to support this, I now consider how the BN model would be used to support the taking of safety related decisions. The analyst might be the safety manager, or other decision maker within the industry. The uses of the model produced, and the improvements and advances that the model and associated tools would bring to risk assessment and safety management in the UK railway industry, are considered.

As argued in section 3.7.3, the process of safety analysis has benefits above and beyond any numerical output that it produces, as it ensures that the domain experts think about the relevant issues in a systematic and structured way before reaching any judgment about what measures to put in place.

The benefit of a risk model is not just in its ability to undertake calculation. The model provides a means of understanding how accidents might occur and therefore how to deal with them. In the following sub-sections the qualitative benefits of using this type of model to support safety decision making are argued.

9.3.1 Analyst view of the model

Figure 54 shows an overview of proposed views produced when condition information is entered into the model using the running example from section 9.1 as its basis. Note that the fault tree and event tree are simplified versions of the extended fault and event trees shown in Figure 49 and Figure 50. When a particular set of conditions has been entered into the model some of the branches of the extended trees may become redundant. Figure 49 shows that under the conditions entered in the illustrative example outcome five becomes impossible. Therefore, the view of the resulting event tree can be pruned to a more simple structure as shown in Figure 54. Similarly Figure 50 shows the event two is not possible and under these conditions the fault tree shown here is simplified to a single AND gate.

The views shown in Figure 54 are complementary. The standard fault and event tree views, which are familiar to industry risk analysts, are presented. However they are annotated to explicitly identify the condition states which comprise the underlying assumptions of the model. The BN model provides an alternative causal model of the same phenomena which shows the causal relationships between all events and conditions.

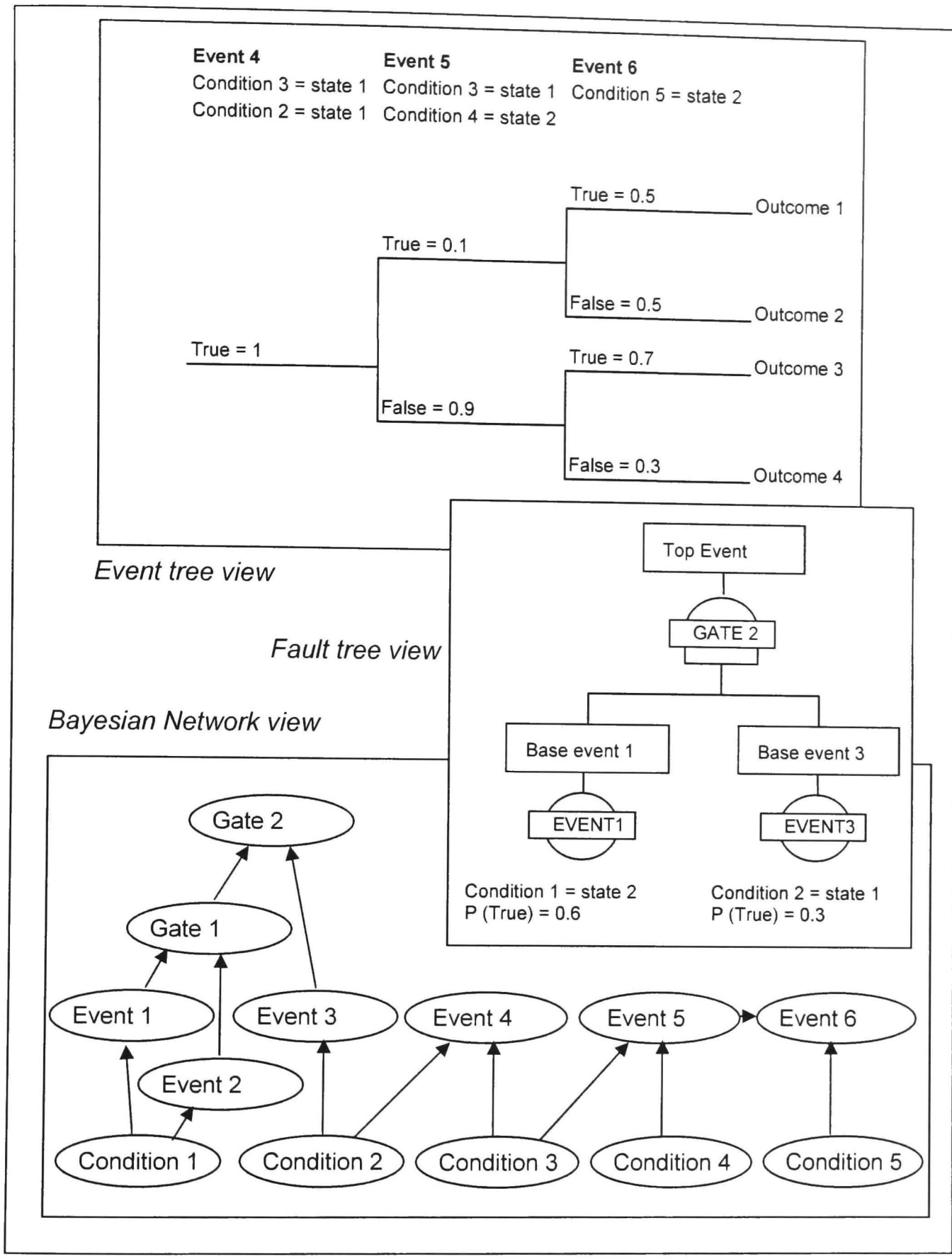


Figure 54: Fault tree and event tree views: Condition information entered

9.3.2 Improved causal model

The BN view of the model offers a view of the causal mechanisms that are implicated in the occurrence of possible accidents that is complementary to the fault and event tree views. The BN view of the model explicitly includes conditional probability relationships between events. This should make it less likely that such relationships are missed or erroneously included. The model also explicitly shows the causal

relationships between events and conditions. This richer causal model should help the model architect to more easily capture the actual causal phenomena that they believe exist in the real world.

9.3.3 Stable, trusted and shared models of risk

Another key advantage of the BN model is its re-usability. The model would be re-reviewed and refined over time. The model captures the fundamental events and logic that are implicated in the occurrence of accidents. Because these aspects of the model are translatable to any organisation involved in the management of the railway network, the model can potentially be shared between organisations. In this way it could be used to consolidate and share knowledge.

In many railway companies, there is no internal resource dedicated to risk analysis and modelling. Consultants tend to be employed, as was the case with the core derailment study. This acts as a disincentive against the use of risk models to support decision making. The user of the BN model, the analyst, does not require any specific knowledge or experience in risk modelling other than an ability to understand and interpret the causal models. A model of this type could shift the focus away from actually doing the analysis to interpreting and understanding the results. The user does not have to be an expert at constructing models. The user would only need to input the condition states of relevance and would need to be competent in the understanding and interpretation of the improved causal models produced.

9.3.4 Modelling of conditions

Standard approaches, like those reviewed in section 4, do not compel the analyst to consider relevant conditions and assume that the analyst will manually document them as assumptions. Using the model and the methodology outlined here conditions are explicitly included. The author of the core derailment study commented that:

'Even though in the derailment report many of the assumptions are documented in detail there are still some things which, now I look at the report after some time, are only implicit in the model. The BN looks as if it makes these factors explicit.' (appendix A2).

The model development includes a stage ('add conditions' in the description of the method) where the editor must consider which conditions are relevant to each event. The result is a clear graphical model of the conditions which influence the probability of

each event. Figure 53 shows the set of conditions influencing the event 'track fault detected'.

The methodology ensures that probabilities of occurrence of 'track fault detected' can only be entered when each of the conditions is set to a particular state. This makes the context in which the probability is estimated clear avoiding any ambiguity in probability estimates.

The use of correlation charts prompts the editor to consider correlations between all events and any conditions modelled too. This type of analysis is again not prompted by existing methods. Conditions might introduce correlations between events in the same part of the model or between events in the fault and event tree parts of the model which are usually modelled separately and in which inconsistent assumptions might easily be made. Section 4.3 described how the value of speed was assumed to be different in the fault and event tree parts of a model produced for an industry study. Using the approach outlined here, it is impossible to assume different condition states in different parts of the model as the states are set in a single place.

9.3.5 Accessible to, and understandable by local managers, decision makers, policy makers and strategic decision makers

The approach outlined in this section uses fault trees and event trees as a specification from which to generate the BN model. The review described in section 6.4.3.1 found that others had identified that BN models are visually difficult to comprehend as little structure is imposed on them by the modelling approach itself. In some of the models presented in this chapter nodes and arcs were removed to make the diagrams easier to understand. The core derailment study risk analyst found it difficult to interpret the meaning of the BN event tree model produced (Figure 34) and commented that one of the reasons why event trees are widely used and trusted in safety engineering is that they are conceptually simple and easy to understand. For these reasons the decision was made to develop the BN from fault and event trees. This aids in the interpretation of the BN model, which could also be presented with clear links between the two contrasting models shown. The BN can be considered to provide an alternative view of possible accident causal sequences. At the core of any model built using the approach described is an accepted and widely understood model of accident sequence. This approach was chosen deliberately. There is no point in an organisation having a completely accurate and infinitely flexible model of risk if that information is not translated into effective and timely practical decisions throughout the industry. One of the key reasons why fault and event trees were chosen as the basis of the model is

that they form part of the common language of the UK railway safety engineering community, and this will help to make the model accessible to those who must use its output to inform management decisions. The approach also retains existing safety engineering structure and terminology. For example, the concept of a hazard, and of various levels of cause, is retained.

Having seen the BN model produced, the analyst believed that the more explicit modelling of assumptions that is supports, and the elicitation process necessary to produce such models could lead to more effective and consistent handling of model assumptions.

The approach was also reviewed by the manager of the Safety Management Systems Programme at RSSB (see Appendix D), who commented:

'*Speaking as an industry Safety Manager who has had first hand experience of developing high level organisational risk assessments using existing industry modelling techniques, I found the concepts proposed extremely thought provoking and easy to understand, and as such can certainly visualise their practical application..*'

9.3.6 Review against SDM1

The risk modelling approach here builds on existing safety management concepts, terminology and models. It therefore provides a model which is understandable by all of those who currently undertake quantified risk assessment in the industry. However it extends existing practice to make the assumptions that underpin that practice more transparent. It also provides an alternative model that helps in the understanding of the causal relationships that underpin current approaches. Updating of the model to calculate revised risk estimates would require no expertise in risk assessment as it is purely a question of setting conditions (like line speed and track curvature) to their proposed state. When compared to existing approaches the model is more accessible to and understandable by those who actually manage safety on the network and therefore substantially meets requirement SDM1.

9.4 Chapter summary

In this chapter, I described how parameterised BN models of the type described in Chapter 8 would be developed and used in practice. I then argued that the model, as described, partially meets SMS1, and provides the foundation for development to meet this requirement more fully (this will be further investigated in sections 10.4.1 to 10.4.3). I also argued that, when compared to existing approaches the model is clearly more

accessible to and understandable by those who actually manage safety on the network and therefore substantially meets requirement SDM1. Having previously concluded that the models met requirements RMR1-RMR3, I can now conclude that Hypothesis 4 is valid (i.e. that the development of a risk modelling approach that possesses the characteristics proposed in Hypothesis 2 is possible).

10 Conclusions, contribution and further work

In this chapter, the argument put forward in this thesis is restated in summary form. The contribution of the work described here is then put forward, making reference to other related work. Further work and areas of research opened up by the research described here are then outlined. Finally I consider the concept of a parameterised risk model and what the future might be for this type of modelling approach.

10.1 Conclusions: Summary of argument

The argument presented in this thesis is reprised in this section. Each of the hypotheses that were initially presented in section 1.4 are considered in turn, and the arguments in support of them summarised.

Hypothesis 1 'Organizational accident theory provides an explanation for the mechanisms by which major accidents occur within the UK railway industry'

According to (Reason 2002), complex safety critical systems are prone to the occurrence of organizational accidents. Organizational accidents occur when multiple safety controls fail at the same time, in the same location. In Chapter 3, I reviewed the recent accident history of Britain's railways and found that organizational accident theory explains many of the phenomena seen in the industry. The theory provides an explanation of the causal mechanisms by which the Ladbroke Grove accident occurred, and how its various causes arose. It also describes the industry's response to major accidents more generally and provides an explanation for trends seen in reported accident levels in the industry.

Hypothesis 2: Given that the industry is prone to the occurrence of organizational accidents a risk modelling approach with particular characteristics is needed in order to ideally support the effective management of safety.

The safety controls that must fail in order for organizational accidents to occur are implemented to prevent the occurrence of events in the accident event sequence, and also relate to the underlying causes that influence the likelihood of occurrence of these events. In section 2.3.2, I categorised these underlying causes as technical, operational and organizational conditions. Risk on the railway industry is also closely related to the performance parameters of the network such as the density of traffic and speed of trains. These parameters were categorised as performance conditions. The categorisations link organizational accident concepts to related risk modelling

terminology and concepts and therefore provide a solid basis for the development of a risk modelling approach that applies the principles of organizational accident theory.

In section 3.6.3, I argued that the nature of the UK railway network meant that it experienced particular problems with the management of organizational accidents. The UK railway network exists over a wide geographic area. Similar hazards are possible at many different locations across the network. However the various underlying accident causes – the condition states – vary greatly depending on the particular location and the time of day, week or year. In addition I argued that risk on the network was likely to be unevenly distributed with 'risk hotspots' existing where the conditions for an organizational accident were substantially in place. Risk estimates from the railway industry support the hypothesis that such hotspots exist (see section 3.5.2). This creates a management problem for the industry.

This implies that in order to ensure safety and prevent the occurrence of organizational accidents the industry needs to be aware of all condition states across the network at any given time. The industry also needs models that allow them to analyse these conditions states and interpret their relationship to accident risk. On this basis I proposed ideal requirements for risk models to support the management of safety in the UK railway industry. These were:

RMR1: Risk models should allow for as many of the events in an accident sequence to be modelled as is practicable.

RMR2: Risk models should allow as many of the significant and quantifiable technical, operational, organizational and performance conditions that cause accidents or exacerbate risk to be explicitly modelled as is practicable.

RMR3: Risk models should be parameterised by conditions so that the risk at different locations and in different situations on the railway network can be rapidly recalculated.

I argued that risk models and information need to be presented to safety professionals in a form that they understand and in a way that allows them to make effective decisions about how to manage safety and proposed two additional requirements on this basis:

SMS1: In order to ensure that they effectively support the management of safety, the uses of a risk model should support the various stages of a safety management system.

SDM1: In order to ensure that they effectively support the taking of safety related decisions, risk models should be usable and understandable by those who actually manage safety on the network.

Hypothesis 3: Current risk modelling approaches in use in the UK railway industry do not have these characteristics.

In Chapter 4, I argued that existing risk models (section 4.2.1) and risk modelling approaches (sections 4.1.1 and 4.3.2) in the UK railway industry do not have the ideal characteristics outlined and substantially fail to meet requirements RMR1-RMR3. In particular, I found that modelling approaches do not provide a full model of the accident event sequence. Fault and event trees are commonly used and this approach does not include explicit modelling of condition states instead documenting them separately as assumptions. I also found that models are developed with a wide scope and average or worst case condition states are assumed, meaning that the applicability of the models to particular situations is unclear. In existing models (section 4.2.1) and in research undertaken (section 5.3) attempts had been made to take account of a wider range of condition states in risk models but this results in increased fault and event tree model size as each unique combination of conditions requirs additional fault and event tree models to be produced. The industry risk model, the SRM, also suffers this problem with additional instances of fault and event trees required to model each separate unique set of condition states (section 4.2).

Hypothesis 4: The development of a risk modelling approach that has these characteristics is possible.

From a review of the state of the art in risk modelling, I found that rapidly updatable, parameterised risk models are used in other industries (section 5.4). I also found that work had already been undertaken on the Irish railway network (section 5.2) which partially met the requirements set out. Also, in the aviation sector some models had been developed or were under development which used BNs to incorporate condition states directly into risk models (section 6.4.3). The review led to the conclusion that BNs provide a technique which is flexible enough to be used to include a variety of condition states in a risk model. However, it would be sensible to develop a method which used the structure of fault and event trees to build the BN model. This would help safety professionals in the railway industry to be able to interpret and understand the BN model and hence would help the model to meet requirement SDM1.

Previous research had described how to translate fault trees into equivalent BNs (section 6.4.4). Chapter 7 showed how to translate a generic event tree structure for a

particular hazard into a BN. By adding condition nodes and eliciting conditional probability relationships a model is produced which allows the generic model to be made more specific by setting the states of conditions. An existing case study supplemented by the judgement of its original author was used to illustrate how the approach would work. Chapter 8 expanded on this case study by including a BN representation of the fault tree to develop a parameterised bow-tie model. By entering sets of conditions similar to those in which major accidents are known to have occurred, I demonstrated that the model would have identified these locations as having higher probabilities of major railway accidents occurring than a typical railway location. I argued that the model substantially met risk modelling requirements RMR1-3 (section 8.12) with the key exception being that I have not demonstrated how organizational conditions could be included in the model. As will be discussed in the further work section of this thesis (section 10.3.1) there is potential to extend the technique to address this omission.

In Chapter 9, I formalised the modelling approach describing how models of this type would be developed and used. I proposed that software would be needed to make the building of these types of model practical and proposed useful views of the BN and its fault and event tree equivalents to aid in the development and use of the model. The approach was reviewed against the risk modelling requirements.

I assessed the extent to which the modelling approach and models of the type proposed would meet the detailed requirements for models to support safety management systems outlined for requirement SMS1. I argued that the approach substantially meets the requirements which align with the organisation and planning elements of a SMS. The approach partially meets the requirements that align with the other elements of a SMS.

Finally I argued that the model would provide better support for safety decision makers than existing techniques (SDM1) as it produces a model with transparent assumptions, and could be used by safety professionals who are not expert risk analysts.

10.2 Summary of contribution

In this thesis I have developed a new type of risk model, and supporting development methodology, that are aligned to the particular problems facing safety management in the UK railway industry, these problems being:

- Susceptibility of the railway industry to 'organizational accidents'

- The inherent variability in risk across the UK railway infrastructure depending on the set of condition states in any location at any given time.
- The ability of risk models to be used and understood by safety professionals to support their various management activities.

In order to achieve this overall contribution, a number of intermediate contributions have also been made. These are spelled out in the remainder of this section.

- Formulation of a set of requirements for risk models in the UK railway industry

From a review of safety management and safety performance in the UK railway industry, and a consideration of its relationship to organizational accident theory, a clear set of requirements for risk models has been developed.

- Development of a classification of accident cause that is consistent with risk modelling techniques and methods

In section 2.3, I outlined a classification of the causes of accidents, based on a distinction between events and conditions and their sub-types. This classification extends the causal definitions used in organizational accident theory, and is presented to be consistent with risk modelling concepts and terminology. This classification is therefore the fundamental initial step in the development of a QRA approach that is consistent with organizational accident theory. These definitions underpin the whole thesis, and the modelling approach that has been developed.

- Development of a modular way of structuring fault and event trees which prevents the need to replicate logically similar fault and event tree models.

I have developed a new way of encoding all fault and event tree logic in a single BN model, in a way in which the location specific logic and probabilities can easily be recovered and used for the purposes of assessing risk in a particular set of circumstances. This prevents the need to develop a separate fault and event tree for each possible combination of condition states that might exist on a railway network. Standard approaches like the SRM are based on producing separate instances of fault and event trees, and this puts practical limits on the degree of parameterisation that can reasonably be modelled. The model developed by Sotera addressed the problem by separating the Irish railway network into 227 different locations where similar conditions are assumed to exist. Using the approach described here, it is practically possible to build models with a much higher degree of parameterisation than this. For example, the model described in this thesis is capable of estimating risk given

approximately 620,000 different sets of conditions that might exist at any given location or time.

Ale et al (Ale, Bellamy et al. 2006; Ale, Bellamy et al. 2007) apply a similar approach to the model development, using event sequence diagrams and fault trees as part of the underlying BN specification resulting in the development of a single integrated BN similar to the model that is described in Chapter 8. However the airport accident causal model they describe is primarily driven by the need to understand the variability in and complexity of causes of air traffic accidents at a particular airport rather than variability in risk across multiple locations. The focus of this work on the risk at a particular airport contrasts with the focus of this thesis on modelling of risk across a variety of locations on a national railway network. They do not describe the problem of variability across a range of locations and offer no specific solution for it.

- Development of a modelling approach which has the potential to be used to include technical, performance, operational and organizational causes of accidents.

As this logical core of the model is developed in a BN, there is the potential to extend any model developed using this technique to include non-deterministic causes of accidents, such as audit indicators, or qualitative judgements about human performance, as long as some statistical relationship between these causes and existing events and condition states in the model can be established. The model described in Chapter 8 includes technical, performance and operational conditions. In section 10.3.1 I outline ideas for further research to allow the inclusion of organizational conditions in the model.

The uses of the Sotera model reflect its focus on technical and performance conditions. It would be difficult for Sotera to expand the model to include operational and organizational conditions for the reasons that were outlined in section 2.4.2, as it is structured around standard fault and event tree techniques

The BN produced for Schipol Airport primarily extends their model to include variability in human performance, the potential source of most variability in accident likelihood that might be expected at any given airport. The model includes operational conditions, described as performance shaping factors, which are considered to have a significant influence on human error probability, and provides some additional confidence that rigorous inclusion of such causes in a BN model is possible. No parameterisation to capture technical conditions is described in the approach presumably because these conditions were assumed to be fixed, and known within Schipol airport.

- Development of an approach, which presents the traditional fault and event tree logical structure, and its underlying assumptions, in a transparent alternative causal model.

By using BNs to extend fault and event tree modelling approaches, a modelling methodology that builds upon accepted concepts and techniques in safety engineering that are extensively used in the UK railway industry has been developed. The resulting BN provides a qualitative model of the causes of accidents that provides safety engineers and analysts with a conceptual model to support understanding of the causal mechanisms that lead to risk. This model is in addition to, and supplements, the fault and event tree view of this model which is retained, providing methodological benefits to its use, which have the potential to strengthen the link between risk assessment and safety management, and to improve a safety decision makers understanding of risk issues.

The Sotera modelling approach described makes use solely of fault and event trees as parameterisation of the model is undertaken in an additional layer of software, rather than using a BN. Therefore, there is no alternative causal model to aid understanding of the causal relationships than underpin parameterisation. Nevertheless, the model does not reproduce the fault and event trees that result from the instantiation of condition states. This means that the approach does not have some of the methodological advantages of the approach described in this thesis, which were described in section 9.2.

Ale at al do not describe the qualitative benefits of using accepted causal models to provide an alternative representation of the BN in their airport risk model. Neither do they describe the methodological approach and benefits of their approach. Instead they stress the need for the model to produce quantitative output for the purposes of cost benefits analysis, a use which the model described here also support (see section 9.2.4).

10.3 Further Work

In this section, further work to develop and extend the modelling approach described in this thesis is suggested. Consideration is given to extending the modelling approach to support:

- Inclusion of organizational conditions
- Development of network wide risk estimates in the absence of a full set of data

- Diagnostic reasoning
- The specification and collection of monitoring data

10.3.1 Including organizational conditions in the model

I have argued that the modelling methodology proposed in this thesis results in the development of risk models that substantially meet the requirements that were previously set out for an ideal UK railway risk model. A key attribute of the modelling approach is that it results in models in which condition states are both explicit and variable. The derailment model presented in Chapter 8 provided an example of the type of model proposed. However, this model explicitly includes technical, operational and performance conditions only and does not include organizational conditions within its scope.

The inclusion of organizational conditions within the model is necessary to fully meet the ideal modelling requirements that were set out in section 1.4 to align models with the possible causes of organizational accidents. Research has argued that failure in the management of organisations is instrumental to the occurrence of complex accidents in modern industrial systems. It is widely accepted that the Challenger space shuttle accident was the result of organizational failings (see for example (Vaughan 1996; Hall 2003a). The chemical disaster at Bhopal and the Nuclear disaster at Chernobyl are also considered to be the result of organizational failings and poor safety culture (Pidgeon and O'Leary 2000). A review of the Ladbroke Grove railway accident (section 3.3) described how organizational weaknesses were considered to be fundamental causes of that accident. The inquiry report included a whole chapter ((Cullen 2001), pages 59-77) on industry failings at the organizational level.

The Baker Report into the Texas City refinery accident (Baker, Leveson et al. 2007) highlighted how monitoring of the wrong organisational indictors might ultimately result in a lack of focus on the possibility of major accidents. The key finding of that report was that an accident occurred because of a focus within BP on occupational safety – for example slips-trips-and-falls rather than 'process safety'. Linking of organisational indicators to models of possible major accidents, would help to ensure that the purpose and meaning of these different sorts of indicators were not confused.

The risk modelling approach described in this thesis results in the development of a model which incorporates the logic and structure of accepted safety modelling techniques but is implemented in a BN. This provides some flexibility about how the approach might be extended as using BNs any two variables can be linked, as long as

a conditional probability relationship between them can be established. The modelling approach described here results in models displaying a long causal sequence which looks at a range of different events in the fault hierarchy as well as the events following the hazard. If organizational conditions can be found that are correlated to any of these events, then they can in theory be included in the model. As was stated in section 2.3.2.3, organizational conditions like personal attitudes, habits and other intangibles are considered to lead to tangible manifestations that can be used to test and monitor the safety culture of an organisation. Using BNs it might also be possible to link organizational conditions to these tangible manifestations. This would result in a model in which measurements of safety culture could be linked to the underlying accident sequence and hence to estimates of risk.

Further work is required to establish exactly how this might be done. An obvious way forward would be to consider application of existing techniques already proposed by other researchers for modelling organizational conditions using BNs. In the literature review of section 6.4.3, several areas of research were identified where others have proposed how to incorporate organizational conditions into risk models using BNs.

Another approach might be to find a model of the organizational causes of accidents on which to base an extension of the BN part of the model in the same way that fault and event trees, an accepted model of the event sequence, were used as the specification for that part of the model. Initial consideration has been given to some possible approaches. Section 6.4.3 discussed how (Trucco, Cagno et al. 2007) had proposed the use of the structured analysis and design technique (SADT) to structure BNs. (Hale, Heming et al. 1997) have also proposed the use of the (SADT) for modelling safety management systems. The STAMP method (Leveson 2002a) is based around a socio-technical representation of a problem domain showing the safety constraints and hierarchical management structure in place for the operation and development of a technical control system. The model is used to try to ensure that the whole socio-technical system is optimised to prevent the occurrence of accidents. The STAMP method provides a representation of an accident scenario and shows how this is related to the wider system. However, its focus is biased towards technical control systems (and therefore its application) may not be ideally suited to the railway industry application where we are concerned with the wider railway network rather than particular technical systems within it.

Perhaps the most promising model for our purposes is that used within the accimap approach (Rasmussen 1997). Accimap is a qualitative modelling technique to aid understanding of how organizational processes and influences can affect generic

accident sequences. The stated aim of the accimap technique is to represent all of the decision makers (actors), how they interact, and what their individual goals, conflicts and information resources are. Rasmussen argues that, in most cases, the activities of these actors are functionally disconnected, and only the accidents reveal a relational structure. The accimap approach provides a rich model of organizational interactions and how these might impact upon events in the accident sequence. Using an adaptation of the accimap an organizational BN model might be developed made up of:

- Actors: each actor is a role; it is described in terms of its responsibilities relevant to the accident.
- Interactions: these are modelled as the information exchanged between actors.

Measurements that provide evidence for each interaction and its effectiveness could perhaps be identified with the interactions represented as variables in the BN. Data collection and analysis could be used to establish correlations between measured values and the effectiveness of interactions. The statistical relationships between these interaction states and events in the event sequence would also have to be established. This approach is outlined further in (Marsh and Bearfield 2004).

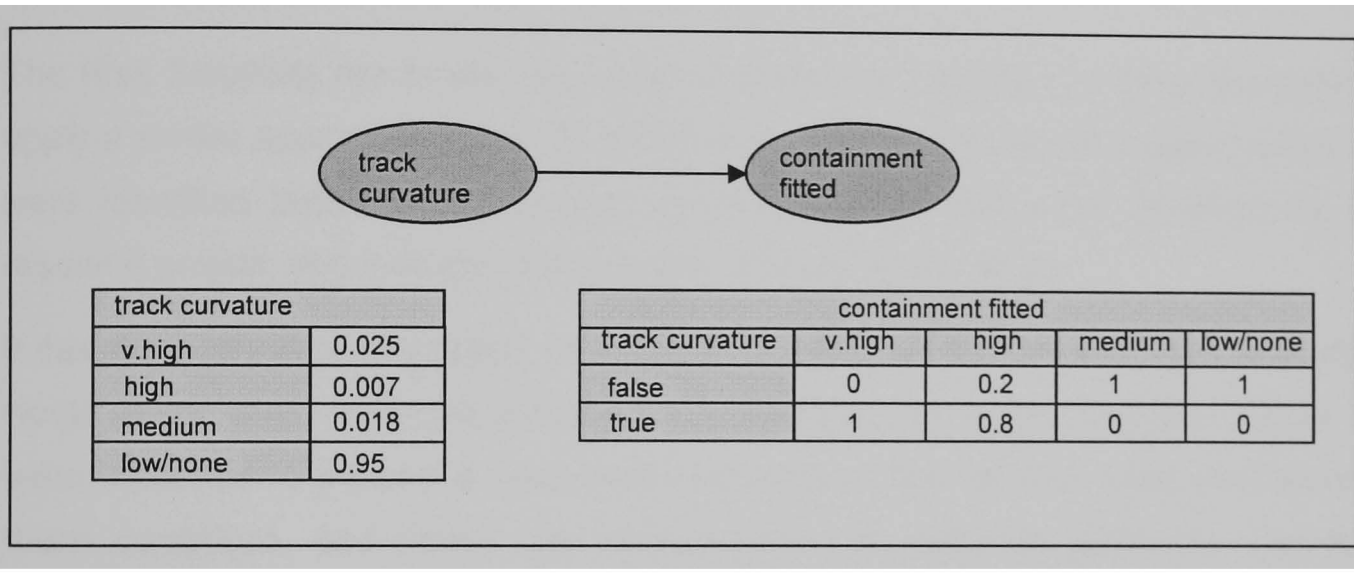
The inclusion of organizational factors in the model would allow the risk estimates to be made that take account of the structure of an organisation and its effectiveness. In theory it would allow safety professionals to identify where poor organizational performance is problematic and possibly a key contributory factor to a high level of risk at certain locations or in certain situations on the network.

This would assist in the structuring and management of organisations to aid risk and safety management. A risk model which included audit findings as conditions could be used to interpret the results of audits, and also to identify areas where audit should be targeted. Audit results and other safety culture indicators could in theory be fed into the risk model on a routine basis to help identify risk hotspots that might emerge as organizational performance degrades over time.

10.3.2 Network wide risk estimates in the absence of a full set of data

Section 9.2.2, explained how the modelling structure and approach proposed in this thesis would make it possible to estimate network wide risk by aggregating the risk from individual locations on the network. However, this would imply that a large amount of data about the condition states, and occurrence of events in each and every location and situation on the network was available, and this is highly unlikely to occur in the foreseeable future.

In the absence of such information the BN may be able to be adapted to provide an estimate of the network wide risk from each hazard. Figure 55 shows two nodes extracted from the BN risk model described in Chapter 8: 'track curvature' and 'containment fitted'. In that model, no prior distributions were set for these nodes. This was not necessary as the nodes were definitively set to a particular state whenever the model was used to calculate risk estimates. However, if it were possible to set these node to represent the distribution of condition states across the network then it might be possible to use the model to approximate risk at the network level rather than just by location. The NPTs shown for the nodes in Figure 55 illustrate how they could be quantified in the risk model in order to do this.



track curvature	
v.high	0.025
high	0.007
medium	0.018
low/none	0.95

containment fitted				
track curvature	v.high	high	medium	low/none
false	0	0.2	1	1
true	1	0.8	0	0

Figure 55: Condition nodes quantified for system wide calculation

The prior distribution for the NPT for 'track curvature' could be estimated taking into account the known properties of track across the network. For example the relative probabilities for track curvature shown have been estimated using data from the Network Rail business plan (NR 2007). The NPT shows that 2.5% of track on the network is considered to consist of 'very high' track curvature (i.e. track curvature with a radius of curvature of 200m or less and 95% with little or no curvature). Estimation of network wide distributions of condition states is a far less onerous task than the collection and population of data for every possible instance of a hazard on the network. However, some condition states are highly correlated to others. Also certain combinations of conditions result in particularly high levels of risk. It is therefore important that the model should take account of the coincidence of condition states, rather than just their distribution; that is, we need to ensure that key correlations between conditions are captured and modelled. Figure 55 shows how this might be done. The state of 'containment fitted' is modelled as having a strong correlation to the state of 'track curvature'. The NPT for 'containment fitted' shows that containment rail is always fitted to rail with severe track curvature, and it is never fitted to rail of medium or

low track curvature. This relationship can be inferred from group standards ((RSSB 2007d) clause 3.2.9), which describe the circumstances under which containment rail is fitted. In the absence of data, a technical expert might be able to estimate that containment rail is fitted to only 20% of rail with 'high' track curvature on the basis of their experience.

By entering the network population distributions into all condition nodes, and including correlations between nodes, the model could be adapted to calculate network wide accident occurrence rates. As the BN model output is in units of events per track mile the output calculations would need to be scaled up by the total number of route miles on the infrastructure[9] to achieve a network total.

The Risk Solutions risk model described in section 5.3 appears to have attempted to apply a similar approach. Figure 20 shows the conditional probability relationships that were identified between the 'environmental' conditions that were identified for that research project, and indicates the strength of these relationships.

If this approach were attempted, one objective would be to determine how the modeller would know when sufficient conditional relationships between condition nodes had been modelled to provide a reasonable estimate of the network wide distribution of these conditions, and hence the network-wide risk estimate given the degree of complexity and variation inherent to the UK railway network. The model would only ever give an approximation of the relationships between condition states and hence of network risk, and therefore ultimately better data collection would remain as the ideal way to enable estimation of network wide risk totals.

Expansion of the model in this way would allow it to be used in a similar way to the SRM (see section 4.2). It would also allow a number of other uses. The user would be able to look at a range of risk profiles that cannot be calculated using the SRM. For example if the model included the same conditions as the BN model in the previous chapter it could look at the network wide risk associated with high speed trains, by setting the line speed node to 'high speed'. By setting the location node, it could calculate the network total risk arising in tunnels; but by setting both, it could calculate the risk arising from high speed trains in tunnels. This ability to consider different types of network wide information would provide additional information to steer network wide decisions and initiatives.

---

[9] There are over 16,000 route miles on the UK rail network according to Network Rail's business plan.

10.3.3 Supporting diagnostic reasoning

BNs are commonly used to diagnose the causes of events (see section 6.4.1). However, to use the model described in this thesis in this way we would need to be confident that the BN inference calculations correctly updated node probabilities when event nodes are set to a particular state. Section 7.3.2 explained that, where an event tree path does not branch, there is insufficient information in the model to determine why this might be. The lack of branching might be because, given the occurrence of preceding events;

- The outcome of the subsequent event is certain, and therefore does not affect event tree outcome probabilities.
- Whether or not the subsequent event occurs is considered by the modeller to be irrelevant to the outcome of that path

As the states of events are not known under certain conditions, it is not possible to assert that events are in a particular state in a coherent way in the model. If the information about the state of events in non-branching paths were known, then it might be possible to use that information to create an event tree in which the state of events could be instantiated into the model.

The event tree in Figure 56 shows a simple, two-event, event tree, the top path of which does not branch. The event tree shows that if event 1 is true, then it is inevitable that outcome 1 will occur. However, given that event 1 is true, the event tree provides no information about the state of event 2. If the translation process as described in section 7.3.1 were to be applied then no causal relationship between event 1 and event 2 would be identified.

Event tree b shows the circumstance where an event outcome is undefined because it is known and considered inevitable given the occurrence of preceding events. In this case a conditional probability relationship exists between events 1 and 2. The event tree has been annotated to show that, given that event 1 is true, it is certain that event 2 is true. If the event tree were to be drawn fully expanded (the alternative view of event tree b in the diagram) it would show clearly that the probability of occurrence of event 2 is conditionally dependent on the outcome of event 1. Hence a causal arc is needed between these two nodes in the BN.

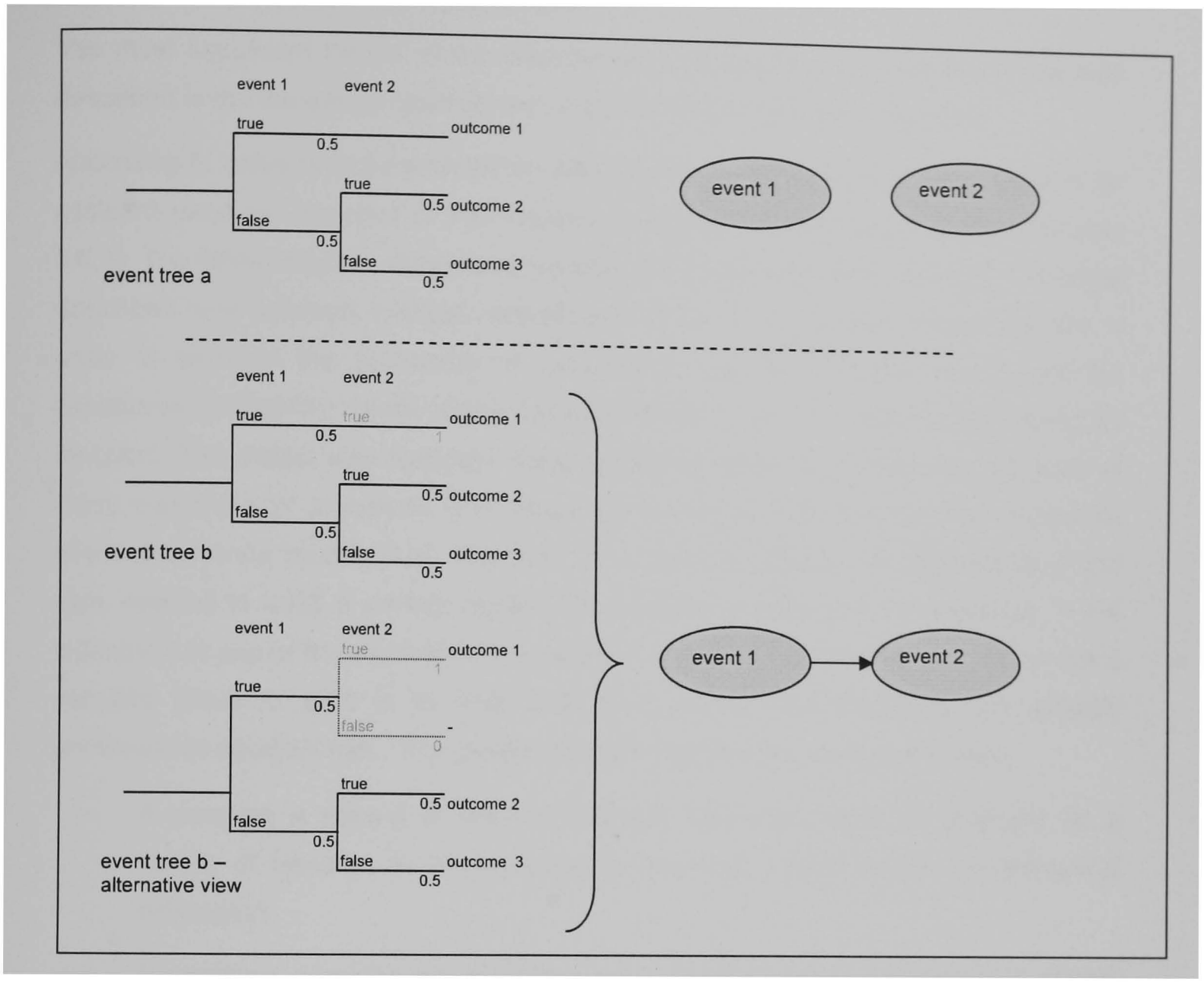


Figure 56: Non-branching paths: Possible reason

The other reason why the path might not branch is that the outcome of the non-branching event is irrelevant to the consequences of that path. This is unlikely as events in an event tree are selected as the events whose occurrence escalates the likely severity of a hazard. In theory, however, there may still be a conditional relationship between one of these 'don't care' events and previous events in the tree. Ultimately if it were possible to annotate the event tree with the full set of possible branches and event probabilities it would be possible to develop a model that included all conditional probability relationships, and therefore in which the state of events could be definitively asserted.

A potential use of such models would be to guide accident investigation and the diagnosis of the cause of an accident.

10.3.4 Data specification and collection

The most significant barrier to the adoption of parameterised risk models of the type described is the increased need for event and condition data that they imply.

According to industry requirements for data collection, only the immediate cause of an accident must be recorded in the industry management information system (section 3.6.1). The SRM structure maximises the use of the available data. However the model described here presents a longer sequence of events in an accident sequence, and in order to estimate the probability of occurrence of each of these events, and the conditional probability relationships between them, a lot of incident data would be required. The model also includes many conditions and this implies that the state of these conditions at any given time should be known in order to infer their impact on event occurrence probabilities. However, the practical difficulty of collecting all of the data needed to build a perfect model only partially undermines the approach. If the industry is to aspire to collect all of the data that is needed to properly understand risk a sensible place to start is to determine what events and conditions are actually correlated to accident risk. The model therefore has two key uses in this area:

- It provides a means of filtering available data that might be collected for a variety of reasons, to identify what is potentially useful for risk modelling and estimation.
- It provides a means of specifying the condition and event data that should ideally be collected (as discussed in 9.2.5). Some of this information might be readily available. The model might also convince a company that, even if some data is difficult to get, it is worth investing the effort in collecting it because it is useful for risk estimation.

The model provides a means of interpreting the data collected and using it to calculate risk. This allows for risk itself to be estimated and monitored and also the model itself provides a justification for detailed incident cause reporting.

By defining the data that would ideally be collected to analyse and assess risk we can start to improve the way in which data is collected in the industry, and over time align and prioritise data collection. The Sotera risk model is the most similar model to the one described here that has been developed and implemented in industry. This model focuses on asset data, asset condition data, and performance data – such as train speeds and train loadings. This information is available and can be collected by surveys and review of planning schedules and information, as it was by Irish Rail to support the Sotera model.

Finally, it should be borne in mind that the model is still usable in the absence of this data. The BN modelling approach reduces any expert judgement problem to the elicitation of the strength of causal relationships between two variables. As we described in section 10.3.2, the model could still be used in practice, even if it were not fully quantified.

10.4 The future of parameterised risk models

Parameterised risk models represent the next natural extension for risk models in the safety domain and in particular in the railway industry. Similar approaches have existed in the nuclear industry for many years, and in this thesis I have reviewed emerging techniques applied in both the aviation and railway industries. Over recent years, safety has improved in the railway industry, and in other safety critical industries. At the same time, the pace of technological change is increasing, placing more and more emphasis on predicting the impact of changed systems and procedures, and on managing the safety associated with their implementation and operation. In the global capital economy, increased efficiency is also needed, meaning that industries will have to ensure that they are prioritising their efforts on safety appropriately and not achieving safety at the expense of performance benefits, or at excessive cost. Risk models which include a greater set of accident causes, both events and conditions, and which can be used to inform management and decision making effectively should be a part of the solution to these problems.

Currently the key barrier to the adoption of fully parameterised risk models as a technique is the availability of sufficient data to quantify the models. In the longer term, this is much less likely to be a problem. Technological advances and the ongoing revolution in the digital economy mean that more data from all sorts of sources is increasingly becoming available over time. In the railway industry there is already increasing use of on track monitoring systems, recording train movements, track cant and levels of adhesion between train wheels and the track. Some trains are also experimenting with real-time transfer of data from trains to control centres. In the years to come it is likely that the problem will not be one of obtaining data, but instead of interpreting and using the myriad of data that is available.

I have previously talked about location specific risk modelling. However, it is only really the physical conditions that could be considered to be a property of a particular location. Other conditions vary over time, and across organisations as well as from location to location. A model that is parameterised to include all condition states would not just be able to differentiate between risk in different locations. It would also be able

to determine the risk relating to different times of the day, week or year. The ultimate vision is of parameterised risk models being used to interpret risk information in real time, and communicate that information instantly to the people who need to act upon it.

11 Glossary

Abbreviation	Description
ATC	Air Traffic Control
ATOC	Association of Train Operating Companies
ATP	Automatic Train Protection
BN	Bayesian Network
DfT	Department for Transport
GEMS	Generic Error Modelling System
HMSO	Her Majesty's Stationery Office
HSWA	Health and Safety at Work etc Act, 1974
LPSA	Living Probabilistic Safety Assessment
MLD	Master Logic Diagram
NATS	National Air Traffic Systems
NPTs	Node Probability Tables
NR	Network Rail
ORR	Office of Rail Regulation
PRA	Probabilistic Risk Assessment
ROGS	Railways and Other Guided Transport Systems Regulations
RSSB	Rail Safety and Standards Board
SADT	Structured Analysis and Design Technique
SCORE	Sensing Changes in Operational Risk Exposure
SMIS	Safety Management Information System
SMS	Safety Management System
SPAD	Signal Passed at Danger
SRM	Safety Risk Model
STAMP	Systems Theory Accident Modelling and Process
TCAS	Traffic Collision Avoidance System

TOC	Train Operating Company
TPWS	Train Protection and Warning System
UK	United Kingdom

12 References

Adams, J. (1995). Risk, Routledge.

Agena. (2008). "AgenaRisk Desktop." from http://www.agenarisk.com/products/desktop.shtml.

Ale, B. J. M., L. J. Bellamy, et al. (2006). "Towards a causal model for air transport safety—an ongoing research project." Safety Science **44**(8): 657-673.

Ale, B. J. M., L. J. Bellamy, et al. (2007). Further development of a Causal model for Air Transport Safety (CATS): Building the mathematical heart. ESREL 2007, Stavanger, Norway, Taylor and Francis.

Asquith (1949). Edwards v the National Coal Board. **AELR Volume 1, 747**.

ATOC (2003). Defensive Driving Principles, Association of Train Operating Companies.

Baker, J. A., N. Leveson, et al. (2007). The report of the BP US refineries independent Safety Review Panel, Available from www.bp.com.

Bayes, T. (1763). "An Essay Towards Solving a Problem in the Doctrine of Chances." Philosophical Transactions of the Royal Soc. of London(53): 370-418.

Bearfield, G. (2007a). "The Route to 'Taking Safe Decisions'." from http://www.rssb.co.uk/pdf/safety/taking_safe_decisions/RouteToTakingSafeDecisions.pdf.

Bearfield, G., P. Dray, et al. (2007). Constructing scalable and parameterised system wide risk models. 25th International System Safety Conference, Baltimore, USA, System Safety Society.

Bearfield, G. J. (2007b). Achieving clarity in the requirements and practice for taking safety decisions in the railway industry in Great Britain. ESREL 2007, Stavanger, Taylor & Francis.

Bearfield, G. J. and D. W. R. Marsh (2005). Generalising Event Trees using Bayesian Networks with a Case Study of Train Derailment. 24th International Conference on Computer Safety, Relaibility and Security (SAFECOMP 2005), Fredrikstad, Norway.

Bedford, T. and R. Cooke (2001). Probabilistic Risk Analysis: Foundations and Methods, Cambridge.

Bedford, T. and J. Quigley (2004). "Risk reduction prioritization using decision analysis." Risk Decision and Policy(9): 1-13.

Bedford, T., J. Quigley, et al. (2004a). Statistical review of the Safety Risk Model: WP1 Report, University of Stratchclyde (for the Rail Safety and Standards Board).

Bedford, T., J. Quigley, et al. (2004b). Statistical review of the Safety Risk Model: WP2 Report, University of Stratchclyde (for the Rail Safety and Standards Board).

Blanks, H. S. (1998). "The Challenge of Quantitive Reliability." Quality and Reliability Engineering International **14**: 167-176.

Bobbio, A., L. Portinale, et al. (2001). "Improving the analysis of dependable systems by mapping fault trees into Bayesian networks." Reliability Engineering and System Safety **71**: 249-260.

Brito, M. and J. May (2006). Gaining confidence in the Software Development Process Using Expert Systems. SAFECOMP 2006, LNCS 4166.

BSI (1999). Railway applications. The specification and demonstration of reliability, availability, maintainability and safety (RAMS), British Standards Institute.

BSI (2001). Railway applications. Communications, signalling and processing systems. Software for railway control and protection systems, British Standards Institute.

BSI (2002). Functional safety of electrical/electronic/programmable electronic safety-related systems Parts 1-7, British Standards Institute.

BSI (2003). Railway applications. Communication, signalling and processing systems. Safety related electronic systems for signalling., British Standards Instiutute.

Buck, L. (1963). "Errors in the perception of railway signals." Ergonomics **6**: 181-192.

CAA (2002). Safety management systems for commercial air transport operations, Civil Aviation Authority.

Campbell, B. and A. Kennedy (2003). Derailment Risk Model (Track Faults): Phase 1 Report, Risk Solutions (for the Rail Safety and Standards Board).

CSNI (2004). Risk Monitors: The State of the Art in their Development and Use at Nuclear Power Plants, Committee on the Safety of Nuclear Installations.

Cullen (2000). The Ladbroke Grove Rail Inquiry - Part 1 Report, HSE Books.

Cullen (2001). The Ladbroke Grove Rail Inquiry - Part 2 Report, HSE Books.

Dahll, G. (2000). "Combining disparate sources of information in the safety assessemtn of software-based systems." Nuclear Engineering and Design **195**: 307-319.

Dennis, C., K. Somaiya, et al. (2002). "The Railway Safety Risk Model." The Journal of the Safety and Reliability Society **22**(3): 39-48.

DfT (2007). Transport Trends: 2007 Edition. D. Anderson and W. Rose, Department for Transport.

DoD (1991). Reliability Prediction Of Electronic Equipment, US Department of Defense.

EC (2004). Directive 2004/49/EC of the European Parliament and of the Council of 29 April 2004 on safety on the Community's railways and amending Council Directive 95/18/EC on the licensing of railway undertakings and Directive 2001/14/EC on the allocation of railway infrastructure capacity and the levying of charges for the use of railway infrastructure and safety certification (Railway Safety Directive), Official Journal of the European Union.

Edkins, G. D. and C. M. Pollock (1997). "The influence of sustained attention on railway accidents." Accident analysis and prevention **29**(4): 533-539.

Evans, A. W. (2003). "Estimating transport fatality risk from past accident data." Accident analysis and prevention(35): 459-472.

Evans, A. W. (2008). Fatal Train Accidents on Britian's Main Line Railways: End of 2007 Analysis, Imperial College, Centre for Transport Studies. Available from www.cts.ic.ac.uk.

FAA (2000). System Safety Handbook: Appendix A, Federal Aviation Authority.

Fenton, N. E., P. Krause, et al. (2001). Probabilistic Modelling for Software Quality Control. Sixth European Conference on Symbolic and Qunatitative Approaches to Reasoning with Uncertainty, Toulouse, France.

Galan, S. F., A. Mosleh, et al. (2007). "Incorporating organizational factors into probabilistic safety assessment of nuclear power plants through canonical probabilistic models." Reliability Engineering & System Safety(92): 1131-1138.

Gran, B. A. (2002). "Assessment of programmable systems using Bayesian belief nets." Safety Science(40): 797-812.

Hale, A., B. Wilpert, et al., Eds. (1997). After the event: from accident to organisational learning, Pergamon.

Hale, A. R., B. H. J. Heming, et al. (1997). "Modelling of Safety Management Systems." Safety Science **26**(1/2): 121-140.

Hall, D. C. and F. P. Wiltshire (2002). Assessment of Railtrack's Management of Multi-SPAD signals, HSE Books.

Hall, J. L. (2003a). "Columbia and Challenger: organizational failure at NASA." Space Policy(19): 239-247.

Hall, S. (2003b). Beyond Hidden Dangers - Railway Safety into the 21st Century, Ian Allen Publishing.

Harper, K. (2000). Safety ideas 'left out of Paddington signals'. The Guardian. Manchester (UK): pp 7.

Harper, K. (2001). Rail boss sacked over lack of drivers. The Guardian. Manchester (UK): p 24.

Heckerman, D. (1990). A Tractable Inference Algorithm for Diagnosing Multiple Diseases. Fifth annual conference on Uncertainty in Artificial Intelligence.

Heinrich, H. W. (1931). Industrial Accident Prevention, McGraw Hill.

Heinrich, H. W. (1951). "Industrial Accident Prevention: A Scientific Approach." Industrial and Labour Relations Review **4**(4): 609.

Heydecker, B. J. and J. Wu (2001). "Identification of site for road accident remedial work by Bayesian statistical methods: an example of uncertain inference." Advances in Engineering Software(32): 859-869.

HMSO (1974). Health and Safety at Work etc Act 1974. (Elizabeth II 1974. Chapter 37), Her Majesty's Stationary Office.

HMSO (1994). Statutory Instrument 1994 No. 237: The Railways (Safety Case) Regulations 1994, Her Majesty's Stationary Office.

HMSO (2006). Statutory Instrument 2006 No. 599: The Railways and Other Guided Transport Systems (Safety) Regulations 2006, Her Majesty's Stationary Office.

Holton, G. A. (2004). "Defining risk." Financial Analysts Journal **60**(6): 19-25.

Hopkins, A. (1999). "The limits of normal accident theory." Safety Science(32): 93-102.

Howes, C. (2001). Thameslink 2000 Programme: Core Section Derailment Study, Railtrack.

HSC (2002). The Southall Rail Accident Inquiry Report: Summary of Progress at February 2002, Health and Safety Commission.

HSE (1997). Successful Health and Safety Management, Health and Safety Executive.

HSE (1998). Report into the accident at Watford South Junction on 8 August 1996, Health and Safety Executive.

HSE (2000). The train collision at Ladbroke Grove, 5 October 1999: A report of the HSE investigation, Health and Safety Executive.

HSE (2001a). Principles and guidelines to assist HSE in its judgement that duty-holders have reduced risk as low as reasonably practicable, Health and Safety Executive.

HSE (2001b). Reducing Risks, Protecting People: HSE's decsion making process.

HSE (2002a). Hatfield Derailment Investigation: Interim Recommendations of the Investigation Board, Health and Safety Executive.

HSE (2002b). The track obstruction by a road vehicle and subsequent train collisions at Great Heck 28 February 2001: A report of the Health and Safety Executive investigation, Health and Safety Executive.

HSE (2002c). Train Derailment at Potters Bar, 10th May 2002 - A Progress Report by the HSE Investigation Board to the end of June 2002. M. Weightman, S. Campbell, M. Roberts and P. E. Shannon, Health and Safety Executive.

HSE (2004). Train Derailment at Ufton Level Crossing near Ufton Nervet, Berkshire: HSE Interim Report, Health and Safety Executive.

HSE (2006). Guidance on Risk Assessment for Offshore Installations.

Hugin. (2008). "Hugin Expert." from http://www.hugin.com/Products_Services/.

IAEA (1999). Living Probabilistic Safety Assessment (LPSA), International Atomic Energy Authority.

IEC (1990). Reliability of systems, equipment and components: Part 7: Guide to fault tree analysis, International Electrotechnical Commission.

INSAG (1991). Safety Culture, International Nuclear Safety Advisory Group.

Isograph. (2007). "Fault Tree Analysis Software - FaultTree+." from http://www.isograph-software.com/.

Jenson, F. (2001). Bayesian Networks and Decision Graphs. New York, Springer.

Joksimovich, V. (1994). Where do we go from here in US nuclear safety regulation? International Conference on Probabilistic Safety Assessment and Management, PSAM II, San Diego.

Kafka, P. (1997). "Living PSA-risk monitoring - current use and developments." Nuclear Engineering and Design(175): 197-204.

Kastenberg, W. E., G. Apostolakis, et al. (1993). A Framework for the Assessment of Severe Accident Management Strategies, NUREG/CR-6056.

Kerh, T. and S. B. Ting (2005). "Neural network estimation of ground peak acceleration at stations along Taiwan high-speed rail system." Engineering Applications of Artificial Intelligence(18): 857-866.

Kim, J. (1973). "Causation, Nomic Subsumption and the Concept of Event." Journal of Philosophy **70**: 217-236.

Kim, J. (1977). "Causation, Emphasis and Events." Midwest Studies in Philoophy **2**(100-103).

Kirwan, B. (2001). "Coping with accelerating socio-technical systems." Safety Science(37): 77-107.

Kirwan, B., R. Kennedy, et al. (1997). "The validation of three Human Reliability Quantification techniques- THERP, HEART and JHEDI: Part 2- Results of validation exercise." Applied Ergonomics **28**(1): 17-25.

Kiwan, B. (1996). "The validation of three Human Reliability Quantification techniques - THERP, HEART and JHEDI: Part 1- techniques descriptions and validation issues." Applied Ergonomics **27**(6): 359-373.

Koornneef, F. and A. R. Hale (2001). How organizations may learn from operational surprises. Fifth International Conference on Technology, Policy and Innovation, Den Haag, Lemma, Utrecht.

Ladkin, P. (2002). Reasons and Causes, University of Bielefield.

Lauritzen, S. L. and D. J. Spiegelhalter (1988). "Local computations with probabilities on graphical structures and their application to expert systems (with discussion)." Journal of the Royal Statistical Society **Series B 50**(2): 157-224.

Lee, C.-J. and K. J. Lee (2006). "Application of Bayesian Network to the probabilistic risk assessment of nuclear waste disposal." Reliability Engineering & System Safety **91**(5): 515-532.

Leveson, N. (2002a). Model-Based Analysis of Socio-Technical Risk, Engineering Systems Division, Massachusetts Institute of Technology.

Leveson, N. G. (2002b). "System Safety Engineering: Back to the Future (unpublished)." from http://sunnyday.mit.edu/book2.pdf.

Lin, J.-H. and P. J. Haug (2008). "Exploiting missing clinical data in Bayesian network modelling for predicting medical problems." Journal of Biomedical Informatics(41): 1-14.

Littlewood, B., L. Strigini, et al. (2000). Bayesian Belief Networks for Safety Assessment of Computer-based Systems. System Performance Evaluation Methodologies and Applications, Boca Raton.

Maglogiannis, I., E. Zafiropoulos, et al. (2006). "Risk analysis of a patient monitoring system using Bayesian Network modeling." Journal of Biomedical Informatics(39): 637-647.

Marsh, D. W. R. and G. Bearfield (2008). "Generalizing event trees using Bayesian Networks." Journal of Risk and Reliability: Part O **O2**(222): 105-114.

Marsh, D. W. R. and G. J. Bearfield (2007a). Merging Event Trees using Bayesian Networks. ESREL 2009, Stavanger, Norway, Taylor and Francis.

Marsh, D. W. R. and G. J. Bearfield (2007b). Representing Parameterised Fault Trees using Beyesian Networks. 26th International Conference on Computer Safety, Relaibility and Security, SAFECOMP 2007.

Marsh, W. and G. Bearfield (2004). Using Bayesian Networks to Model Accident Causation in the GB Railway Industry. 7th International Conference on Probabilisitc Safety Assessment and Management (PSAM7-ESREL4), Berlin, Germany, Springer.

Metcalfe, R. (2006). "Management of SPAD risk - The UK experience." from http://www.halcrow.com/html/documents/pdf/australia/rm_management_spad_risk.pdf.

MOD (2004). Safety Management Requirements for Defence Systems: Parts 1 and 2, Ministry of Defence.

Mosleh, A., E. Goldfeiz, et al. (1997). The w (Omega) - Factor Approach for Modelling the Influence of Organizational Factors in Probabilistic Safety Assessment. IEEE Sixth Annual Human Factors Meeting, Orlando, Florida.

Muttram, R. (2003). UK Railway Restructuring and the Impact on the Safety Performance of Heavy Rail Network. Japan Railway & Transport Review: pp.4–11.

NAO (2004). Network Rail: Making a Fresh Start, National Audit Office.

Neil, M. (2004). SCORE: Sensing Changes in Operational Risk Exposure, RADAR Group. Queen Mary, University of London.

Neil, M., N. E. Fenton, et al. (2000). "Building large-scale Bayesian Networks." The Knowledge Engineering Review **15**(3): 257-284.

Neil, M., B. Malcolm, et al. (2003). Modelling an Air Traffic Control Environment Using Bayesian Belief Networks. 21st International System Safety Conference, Ottawa, Ontario, System Safety Society.

Nikovski, D. (2000). " Constructing Bayesian networks for medical diagnosis from incomplete and partially correct statistics." IEEE Transactions on Knowledge and Data Engineering **12**(4): 509-516.

NR (2007). Network Rail Business Plan 2007.

Oien, K. (2001a). "A framework for the establishment of organizational risk indicators." Relaibility Engineering and System Safety(74): 147-167.

Oien, K. (2001b). "Risk indicators as a tool for risk control." Reliability Engineering and System Safety(74): 129-145.

ORR (2007). Rail Safety: Train Protection and Warning System (TPWS): Fitment at Permanent Speed Restrictions, Office of Rail Regulation.

ORR (2008). Internal guidance on cost benefit analysis (CBA) in support of safety-related investment decisions, Office of Rail Regulation - available from www.rail-reg.gov.uk.

Pearl, J. (1985). "Bayesian Networks: A model of self-activated memory for evidential reasoning." Proceedings: Cognitive Science Society: 329-334.

Pearl, J. (2000). Causality: Models, Reasoning and Inference, Cambridge.

Perrow, C. (1999). Normal Accidents, Princeton University Press.

Pidgeon, N. and M. O'Leary (2000). "Man-made disasters: why technology and organizations (sometimes) fail." Safety Science **34**(1-3): 15-30.

Podofillini, L., E. Zio, et al. (2006). "Risk-informed optimisation of railway tracks inspection and maintenance procedures." Reliability Engineering and System Safety(91): 20-35.

Pullen, R. (2002). "From ESM to RiskVu." from http://www.isograph-software.com/rskoverfsm.htm.

Quigley, J., T. Bedford, et al. (2007). "Estimating Rate of Occurrence of Rare Events with Empirical Bayes: A railway application." Reliability Engineering & System Safety **92**(5): 619-627.

RAIB (2007). Progress Report: Derailment at Grayrigg, Cumbria 23 February 2007, Rail Accident Investigation Branch.

Rasmussen, J. (1997). "Risk Modelling in a Dynamic Society: A Modelling Problem." Safety Science **27**(2/3): 183-213.

Rasmussen, J. and A. Jensen (1974). "Mental procedures in real life tasks: A case study in electronic trouble shooting." Ergonomics **17**: 293-307.

Reason, J. (1990). Human Error, Cambridge University Press.

Reason, J. (2002). Managing the Risks of Organizational Accidents, Ashgate Publishing Limited.

Roelen, A. L. C., R. Wever, et al. (2003a). Aviation causal model using Bayesian Belief Nets to quantify management influence. Safety and Reliability., Swets & Zeitlinger.

Roelen, A. L. C., R. Wever, et al. (2003b). Casual modelling for integrated safety at airports. Safety & Reliability, Maastricht.

RSSB (2001). Guidance on the Preparation of Risk Assessments within Railway Safety Cases, Rail Safety and Standards Board.

RSSB (2002). Guidance on the Preparation of Risk Assessments within Railway Safety Cases, Rail Safety and Standards Board.

RSSB (2003a). Profile of safety risk on the GB mainline railway.

RSSB (2003b). Railway Group Safety Plan, Rail Safety and Standards Board.

RSSB (2006). Profile of safety risk on the GB mainline railway, Rail Safety and Standards Board.

RSSB (2007a). Annual Safety Performance Report 2006. L. Davies, Rail Safety and Standards Board.

RSSB (2007b). Engineering Safety Management, Rail Safety and Standards Board.

RSSB (2007c). Reporting of Safety Related Information, Rail Safety and Standards Board.

RSSB (2007d). Track System Requirements, Rail Safety and Standards Board.

RSSB (2008a). Strategic Safety Plan, Rail Safety and Standards Board.

RSSB (2008b). Taking Safe Decisions.

Sierra, B., I. Inza, et al. (2000). Medical Bayes Networks, ISMDA 2000.

Smith, D. J. (1997). Reliability, Maintainability and Risk, Butterworth-Heinemann.

Smith, J. Q. (1989). "Influence diagrams for Bayesian decision analysis." European Journal of Operations Research **40**: 363-376.

Sotera. (2007). "Developing a location specific risk model for Irish Rail." from http://www.sotera.co.uk/pdf/Location%20specific%20risk%20model.pdf.

Trucco, P., E. Cagno, et al. (2007). "A Bayesian Belief Network modelling of organsiational factors in risk analysis: A case study in maritime transport." Reliability Engineering & System Safety (in press).

Turner, S., D. Keeley, et al. (2002). Review of Railway Safety's Safety Risk Model, Health and Safety Laboratory.

Van-der-Flier, H. and W. Schoonman (1988). Applied Ergonomics **19**(2): 135-141.

Vaughan, D. (1996). The Challenger launch decision: risky technology, culture and deviance at NASA. Chicago, The University of Chicago Press.

Vesely, W. E., F. F. Goldberg, et al. (1981). Fault Tree Handbook, US Nuclear Regulatory Commission.

Watson, H. A. (1961). Launch Control Safety Study, Section VII, vol. 1, Bell Labs, Murray Hill, New Jersey.

Webster, B. (2000). Engineer's rail danger warning. The Times. London (UK): pp 6.

Wilde, G. J. S. (2001). Target Risk 2: A new psychology of safety and health, PDE Publications.

Williams, J. C. (1977). "Railway Signals Passed at Danger - Some Further Research." Ergonomics Abstracts **10**(3).

Williams, J. C. (1986). HEART - A proposed method for achieving high relaibility in prcoess operation by means of human factors engineering technology. 9th Advances in Reliability Technology Symposium, University of Bradford.

Wright, K. (2000). A human factors approach to Investigating signals passed at danger, Human Reliability Associates.

Wright, K. and D. Embrey (2000). Using the MARS Model for Getting at the Causes of SPADs. Rail Professional.

Wright, K., D. Embrey, et al. (2000). Getting at the Underlying Systemic Causes of SPADs: A New Approach. Rail Professional.

Appendices

Table of figures

Tables

Appendix A Urban railway derailment study

A1 Event trees developed for the core derailment study

This section of Appendix A shows the event trees taken from the core derailment study. The consequences of each of the event trees have been numbered so that similar consequences can be grouped in the extended event tree produced as part of the approach described in Chapter 5.

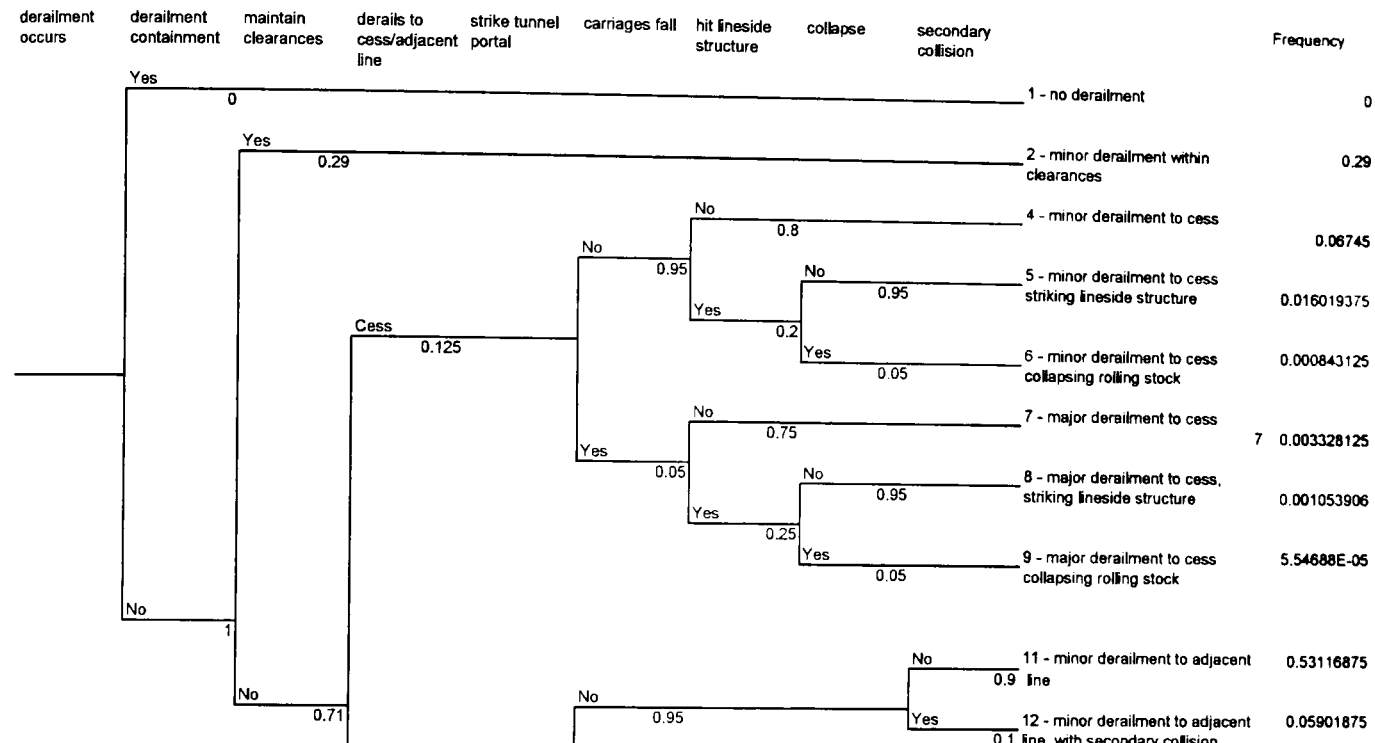


Figure A-1: Event tree for derailment accidents on open track

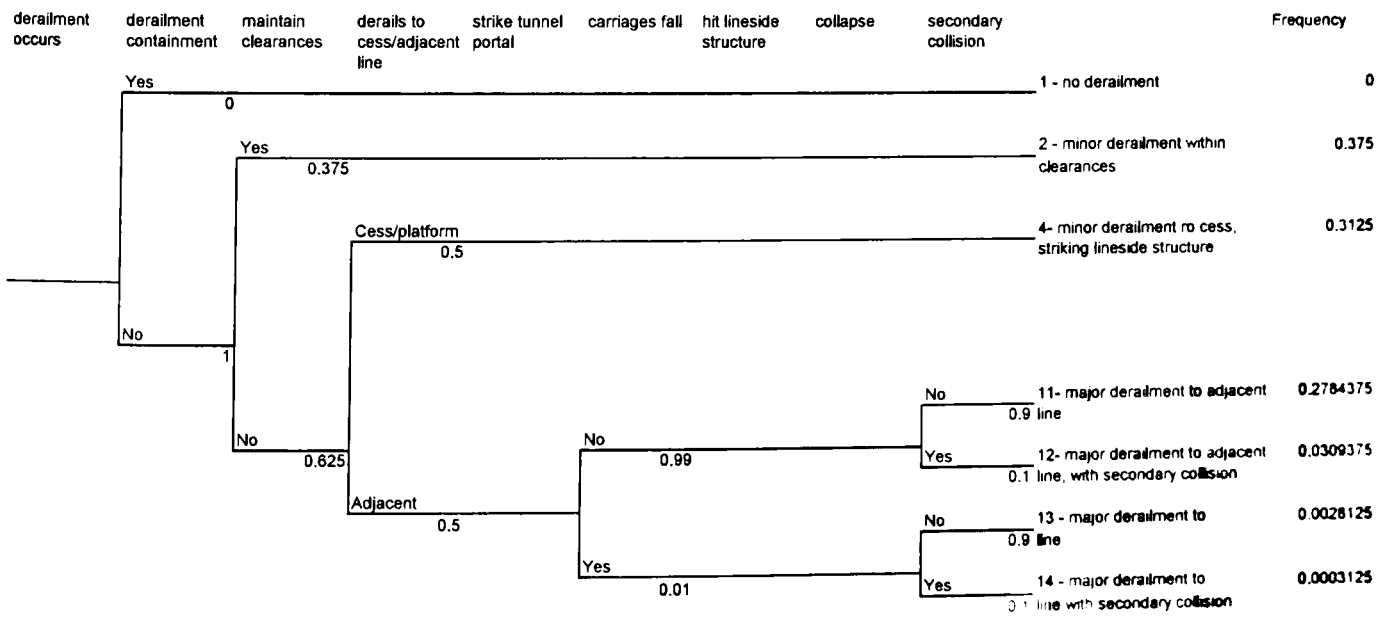


Figure A-2: Event tree for derailment accidents in stopping stations

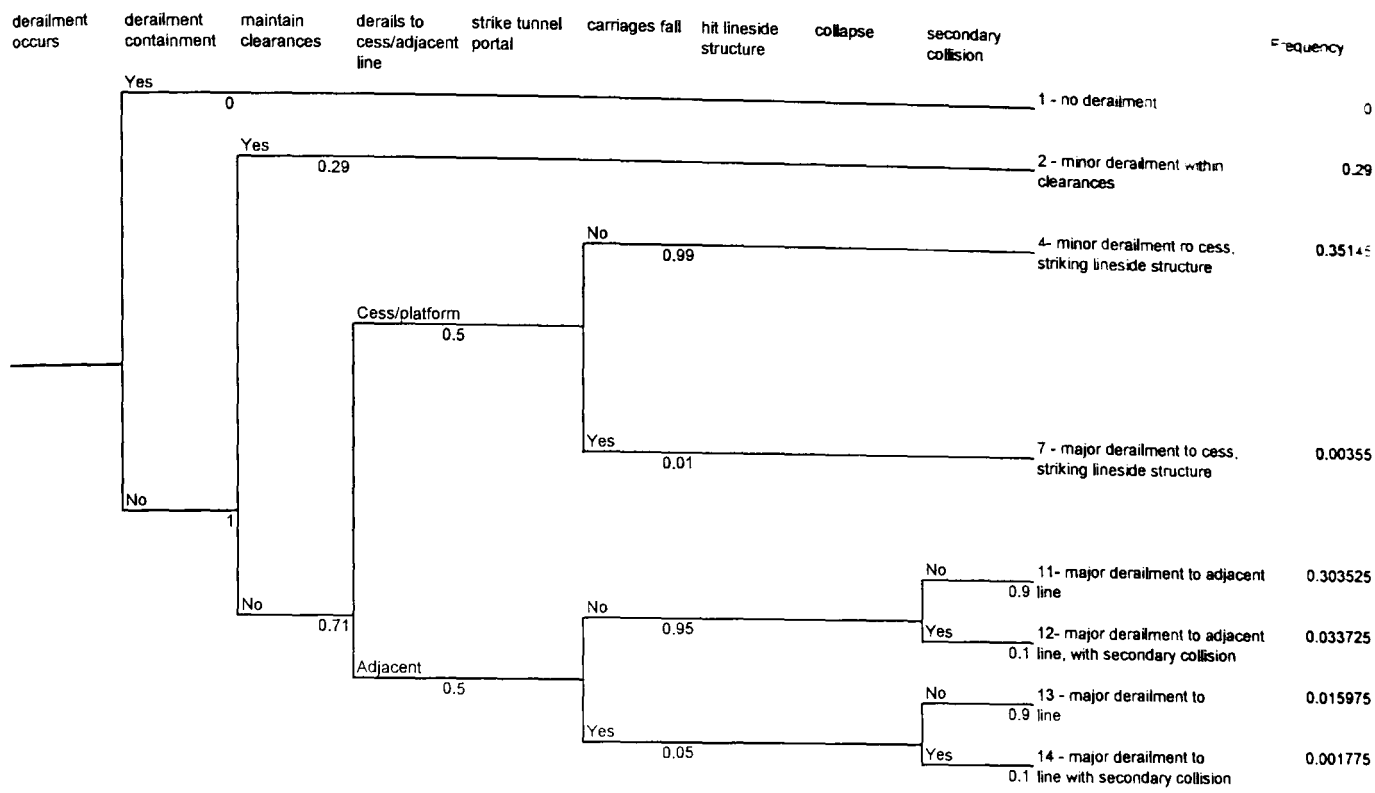


Figure A-3: Event tree for derailment accidents in a twin track tunnel

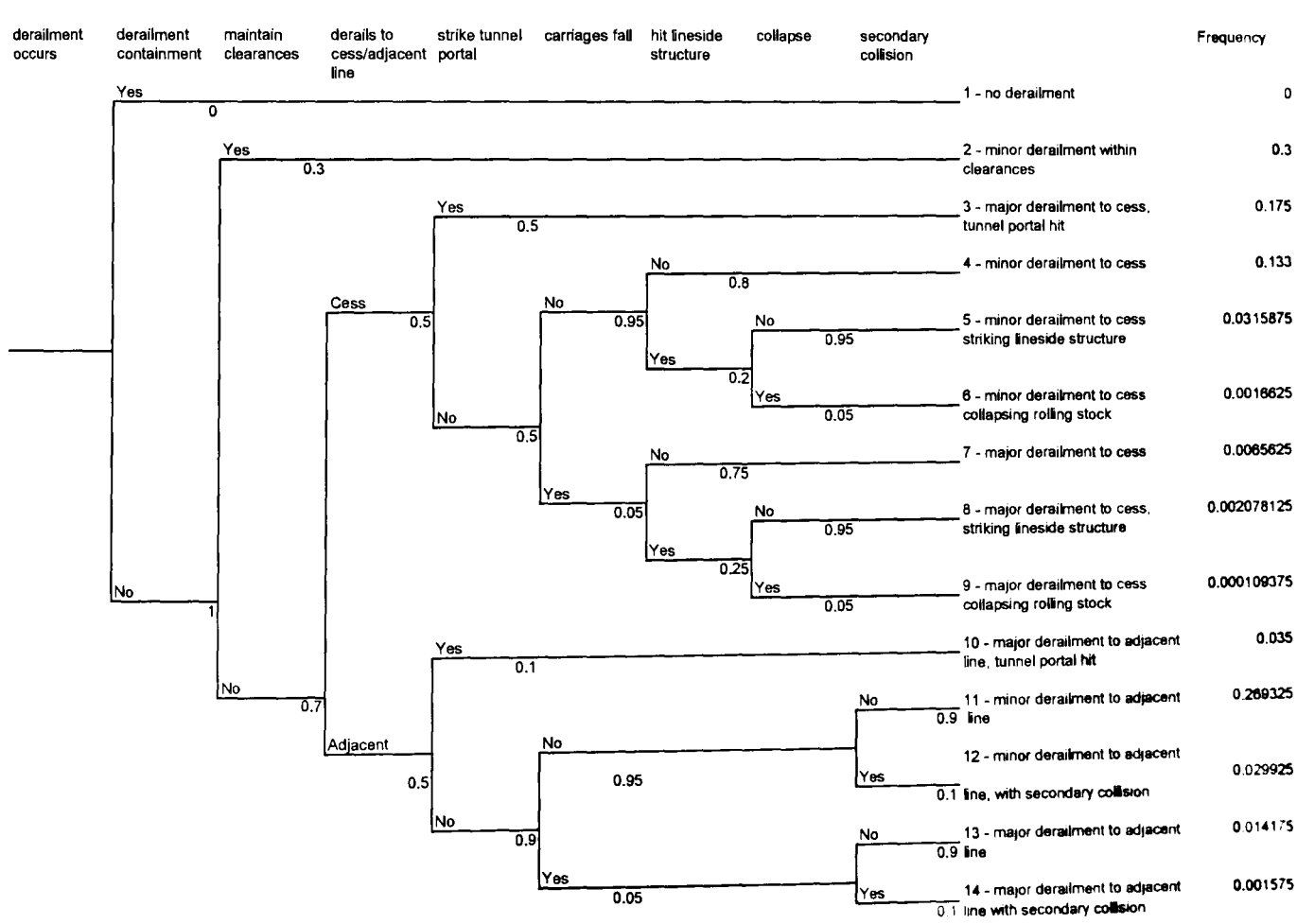


Figure A-4: Event tree for derailment accidents on approach to a tunnel

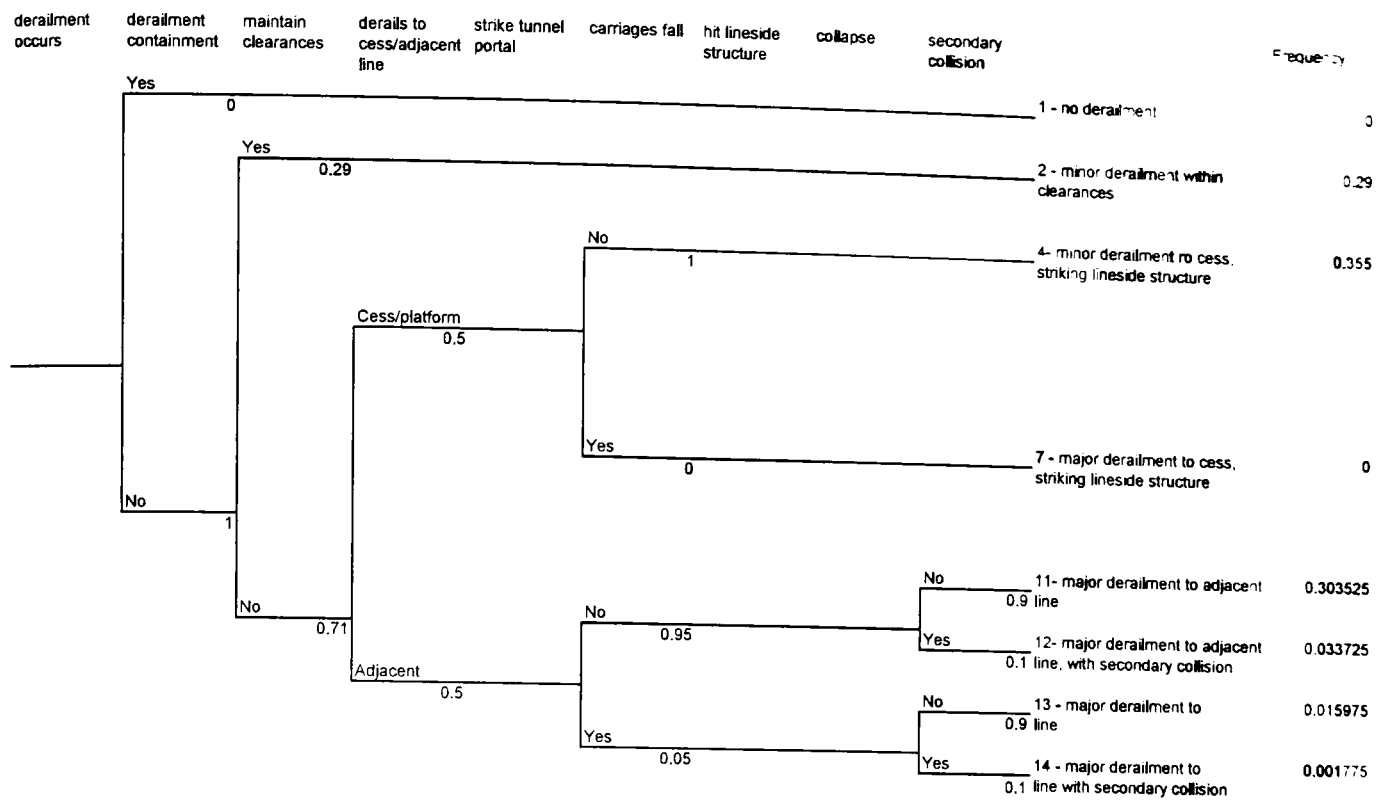


Figure A-5: Event tree for derailment accidents occurring in a station

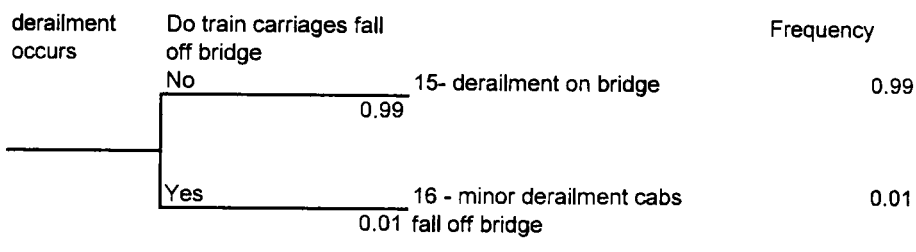


Figure A-6: Event tree for derailment accidents occurring on a bridge

A2 Elicitation meetings to support event tree parameterisation

The expert elicitation required to support the event tree parameterisation exercises described in Chapter 7 took place with the support of Colin Howes of Atkins Rail at three separate meetings on:

- 4 February 2005
- 10 February 2005
- 18 March 2005

Full records of the meetings are available from the author.

Appendix B BN Event tree models

B1 Simple translation from an event tree to a BN

This section of Appendix B describes how to produce a BN version of an event tree, as outlined in section 5.3.

B.1.1 Node Probability Tables

The node probability tables used to quantify the BN model described in section 5.3 are shown below.

Event nodes

Contained

FALSE	1
TRUE	0

Clear

FALSE	0.71
TRUE	0.29

Direction

cess	0.125
adj. line	0.875

Falls

FALSE	0.95
TRUE	0.05

Hits

carriages fall	FALSE	TRUE
FALSE	0.8	0.75
TRUE	0.2	0.25

Collapse

FALSE	0.95
TRUE	0.05

Collision

FALSE	0.9
TRUE	0.1

Consequence nodes

The methodology described in Chapter 5 shows that the consequence node can be produced by creating a single node, whose parents are the full set of event trees.

However, even for this relatively simple example, the NPT produced would consist of 1536 conditional probabilities as there are 7 separate events, each with two states, and 12 possible consequences.

It is therefore easier to build the consequence NPT using a hierarchy of nodes as shown in Figure B-1 below.

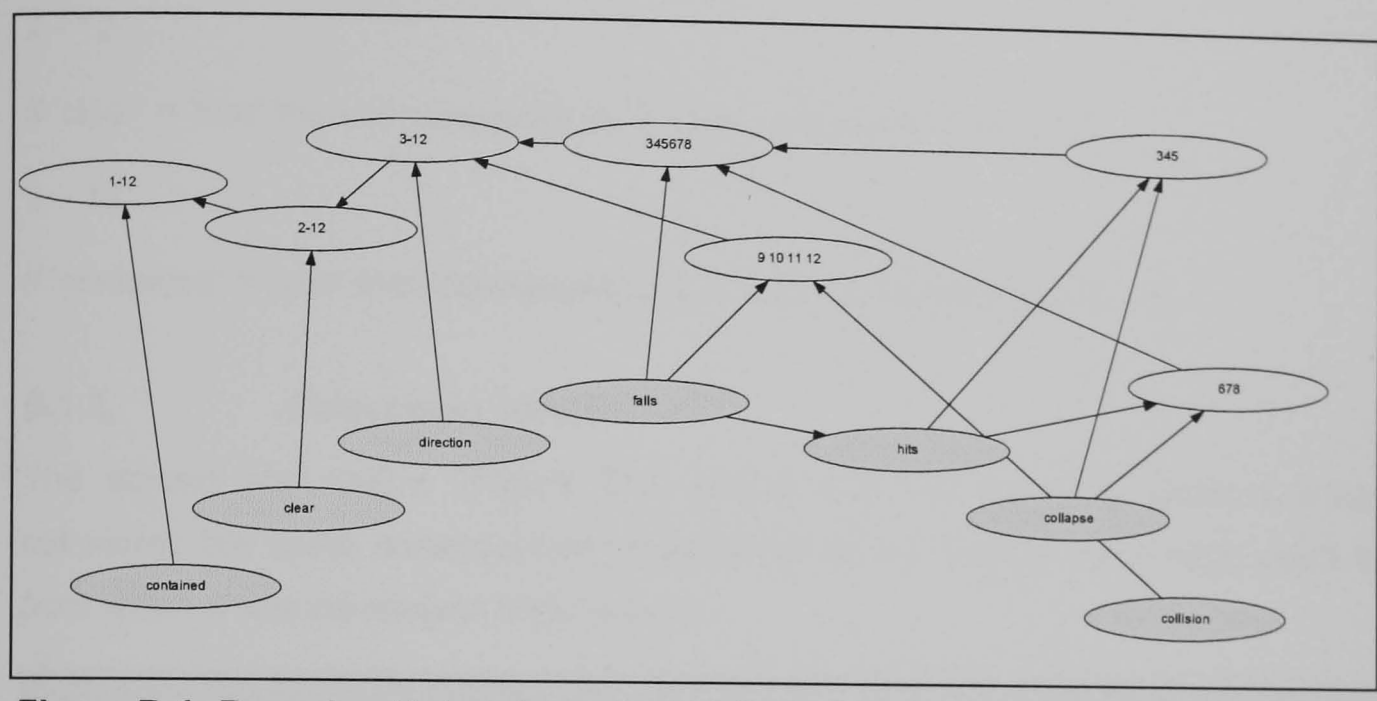


Figure B-1: Bayesian Network version of Open Track event tree

Using a software package like Hugin, it is possible to quantify this hierarchy of nodes using a combination of NPTs and logical statements as shown below:

3 4 5

collapse	FALSE		TRUE	
hits	FALSE	TRUE	FALSE	TRUE
3	1	0	1	0
4	0	1	0	0
5	0	0	0	1

6 7 8

collapse	FALSE		TRUE	
hits	FALSE	TRUE	FALSE	TRUE
6	1	0	1	0
7	0	1	0	0
8	0	0	0	1

9 10 11 12

falls	FALSE		TRUE	
collision	FALSE	TRUE	FALSE	TRUE
9	1	0	0	0
10	0	1	0	0
11	0	0	1	0
12	0	0	0	1

3 4 5 6 7 8

If 'carriages fall' = TRUE then consequence is '678' else consequence is '345'

3 - 12

If 'direction' = 'cess' then consequence is '345678' else consequence is '9 10 11 12'

2 - 12

If 'clear' = 'true' then consequence is '2' else consequence is '3 -12'

1 – 12

If 'contained' = 'true' then consequence is '1' else consequence is '2 -12'

B.1.2 Calculation results

The screen shot below (Figure B-2) shows that the Bayesian Network created calculates the same consequence probabilities as the original open track event tree from which it was developed (Figure A-1).

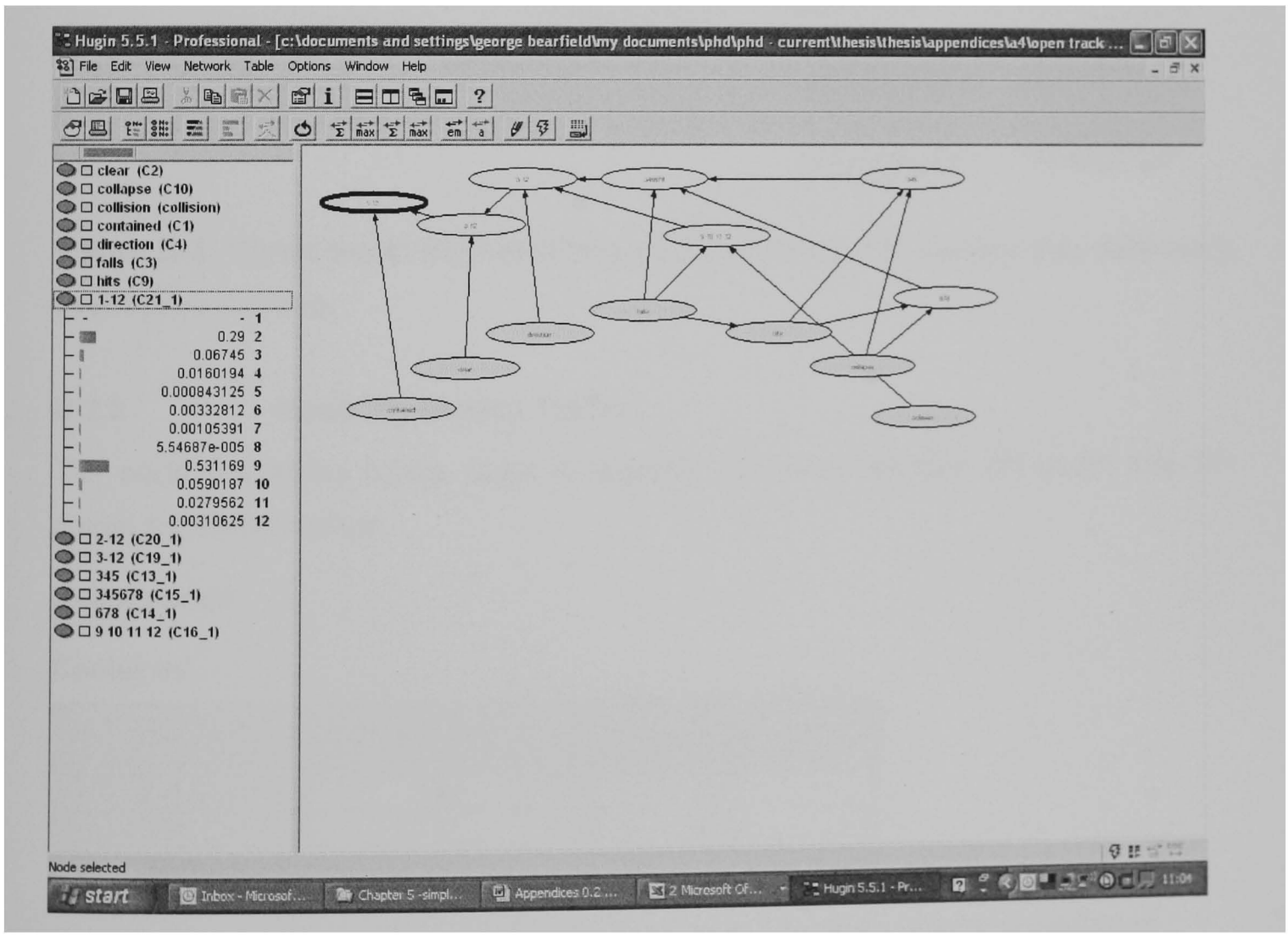


Figure B-2: Screen shot of BN event tree calculation

B2 Parameterised BN Event Tree model

This section of Appendix B shows how a parameterised BN Event Tree model of the type described in section 5.3.3 can be produced.

B.2.1 The BN model

The BN model, expanded to include additional condition nodes is shown below.

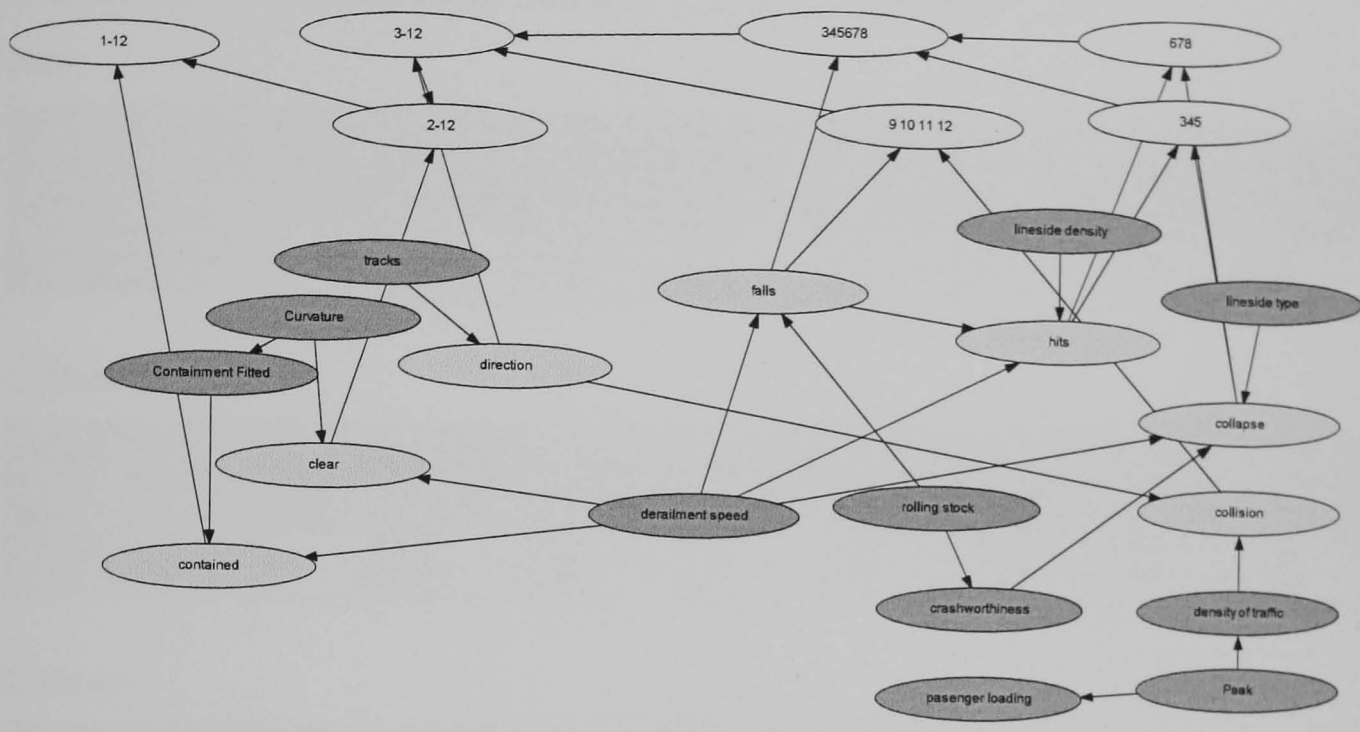


Figure B-3: 'Open track' BN event tree parameterised with factors that determine event probabilities.

B.2.2 Node Probability Tables

The node probability tables used to quantify the parameterised BN event tree BN model are shown below.

Event nodes

Contained

derailment speed	>15		<15	
containment fitted	yes	no	yes	no
FALSE	0.9	1	0.5	1
TRUE	0.1	0	0.5	0

Clear

derailment speed	>15			<15		
curvature	severe	mild	none	severe	mild	none
FALSE	0.71	0.4	0.25	0.625	0.3	0.1
TRUE	0.29	0.6	0.75	0.375	0.7	0.9

Direction

tracks	2	4
cess	0.5	0.125
adj. line	0.5	0.875

Falls

rolling stock	high speed train		emu	
derailment speed	>15	<15	>15	<15
FALSE	0.975	0.9875	0.95	0.975
TRUE	0.025	0.0125	0.05	0.025

Hits

derailment speed	>15				>15			
lineside density	high		low		high		low	
carriages fall	FALSE	TRUE	FALSE	TRUE	FALSE	TRUE	FALSE	TRUE
FALSE	0.8	0.75	0.95	0.9	0.85	0.8	0.98	0.95
TRUE	0.2	0.25	0.05	0.1	0.15	0.2	0.02	0.05

Collapse

lineside type	fixed							
crashworthiness	high		low		high		low	
derailment speed	>15	<15	>15	<15	>15	<15	>15	<15
FALSE	0.85	0.95	0.8	0.9	0.98	0.99	0.95	0.98
TRUE	0.15	0.05	0.2	0.1	0.02	0.01	0.05	0.02

Collision

density of traffic	high		low	
direction	cess	adj line	cess	adj line
FALSE	1	0.9	1	0.99
TRUE	0	0.1	0	0.01

Consequence nodes

The model developed uses the same NPT structure for modelling consequences as the previous model described in B.1.1.

B.2.3 Model output

The two sets of conditions shown in the Table 12 were input into the resulting BN model. One set represents the conditions that might exist on an urban commuter railway; the other represents the conditions that might exist on a high-speed, inter-city type railway.

The accident outcome probabilities calculated are shown in the table below.

Consequence	Probability of occurrence per year		Probability of occurrene per derailment	
	BN model characterised as a commuter railway (column 1 of Table 12)	BN model characterised as Intercity railway (column 2 of table 12)	Commuter railway (as outlined in column 1 of Table 12)	Intercity railway (as outlined in column 2 of table 12)
1	0	0	0	0
2	0.0012267	0.0031725	0.29	0.75
3	0.000285314	0.000489754	0.06745	0.115781
4	6.77621E-05	2.19101E-05	0.0160194	0.00517969
5	3.56219E-06	3.86649E-06	0.000842125	0.000914063
6	1.4078E-05	1.18969E-05	0.00332813	0.0028125
7	4.45804E-06	1.12359E-06	0.00105391	0.000265625
8	2.34633E-07	1.98281E-07	5.55E-05	4.69E-05
9	0.002246845	0.000510375	0.531169	0.120656
10	0.00024965	5.15531E-06	0.0590188	0.00121875
11	0.000118255	1.30866E-05	0.0279563	0.00309375
12	1.31394E-05	1.32188E-07	0.00310625	3.13E-05

Table B-1: Probability of occurrence of derailment on a commuter railway and on an intercity railway (per derailment and per year).

The event tree calculates the probability of occurrence of an accident per derailment. The initial core derailment study calculated that the probability of a derailment per track mile was 4.23E-03 per year. Therefore, the per year consequence probability has been calculated by multiplying the consequence per derailment figure by this number.

B3 Parameterised BN event tree model for multiple locations

This section of Appendix B describes the parameterised BN Event Tree model can be produced that is more general than the models previously described and is capable of calculating the risk is a wide range of different locations as shown in section 5.4 of this thesis.

B.3.1 Extended Event Tree

The extended event tree shown in Figure B-4 was used as the specification for the general parameterised BN event model.

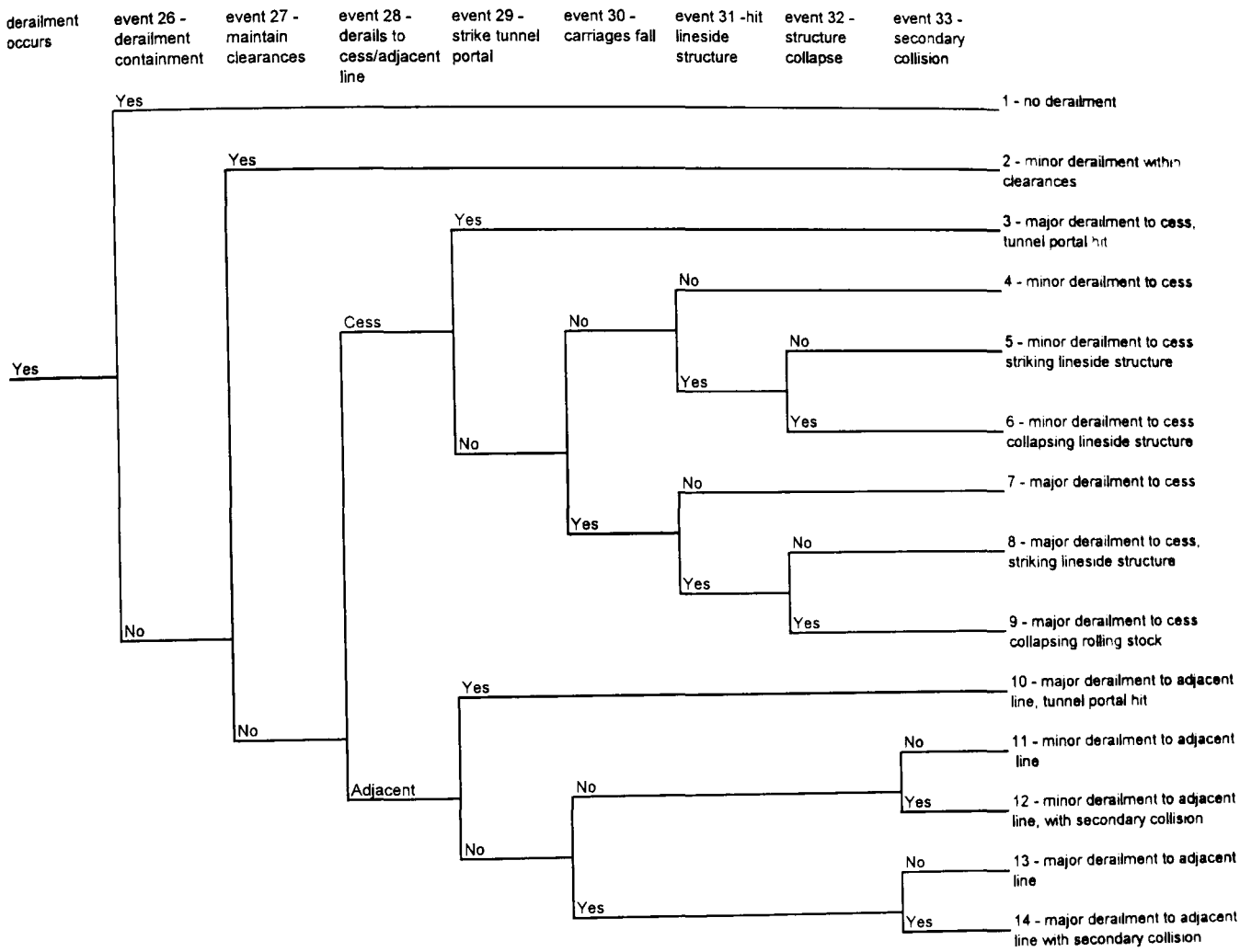


Figure B-4: Extended Event Tree

B.3.2 The BN Model

The BN model produced from the extended event tree of Figure B-4 is shown as Figure B-5. The BN model also shows condition nodes added to parameterise the model.

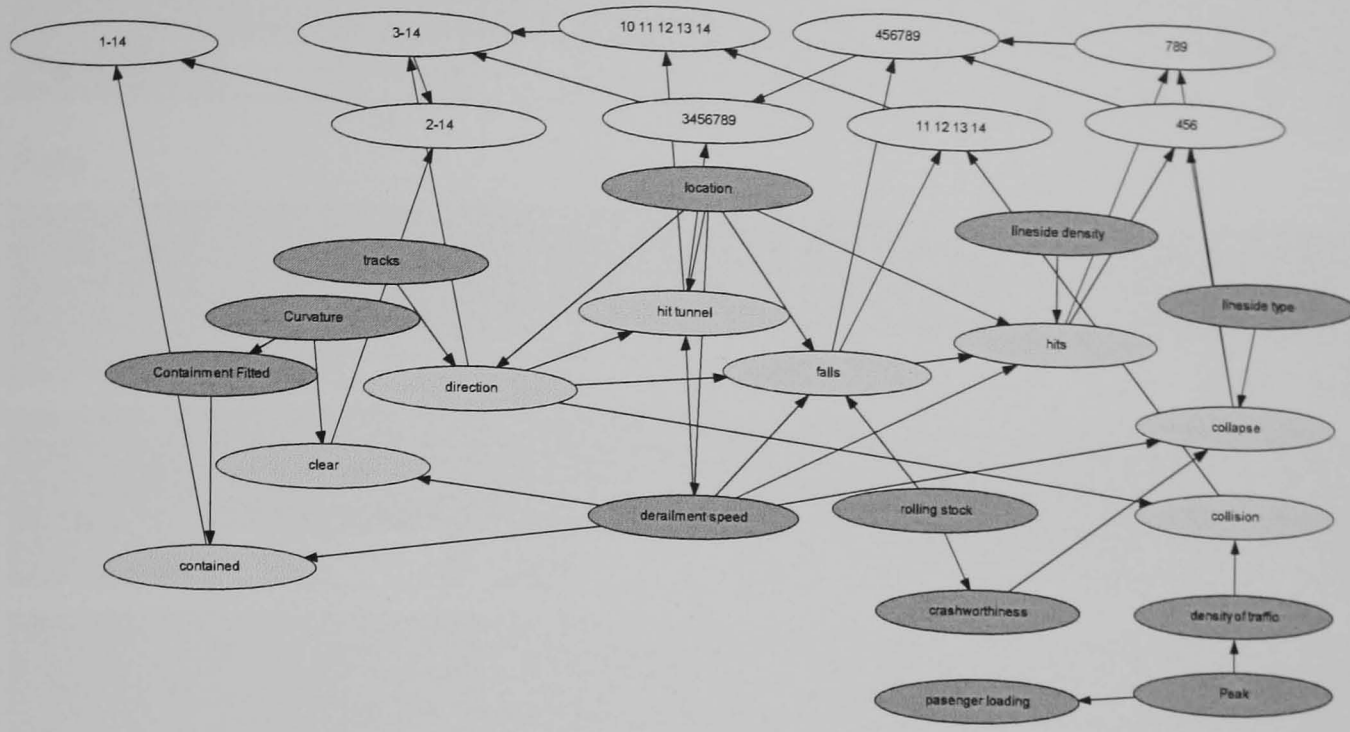


Figure B-5: General BN event tree parameterised with factors that determine event probabilities

B.3.3 Node Probability Tables

The node probability tables used to quantify the parameterised BN event tree BN model are shown below.

Event nodes

Contained

derailment speed	>15		<15	
containment fitted	yes	no	yes	no
FALSE	0.9	1	0.5	1
TRUE	0.1	0	0.5	0

Clear

derailment speed	>15			<15		
curvature	severe	mild	none	severe	mild	none
FALSE	0.71	0.4	0.25	0.625	0.3	0.1
TRUE	0.29	0.6	0.75	0.375	0.7	0.9

Direction

tracks	2					4				
location	open track	in station	tt tunnel	th. station	tunnel app.	open track	in station	tt tunnel	th. station	tunnel app.
cess	0.5	0.5	0.5	0.5	0.5	0.125	0.5	0.5	0.5	0.5
adj. line	0.5	0.5	0.5	0.5	0.5	0.875	0.5	0.5	0.5	0.5

Hit tunnel

derailment speed	>15									
derails to cess/adj	cess					adj				
location	open track	in station	tt tunnel	th. station	tunnel app.	open track	in station	tt tunnel	th. station	tunnel app.
FALSE	1	1	1	1	0.5	1	1	1	1	0.9
TRUE	0	0	0	0	0.5	0	0	0	0	0.1

derailment speed	>15									
derails to cess/adj	cess					adj				
location	open track	in station	tt tunnel	th. station	tunnel app.	open track	in station	tt tunnel	th. station	tunnel app.
FALSE	1	1	1	1	0.7	1	1	1	1	0.95
TRUE	0	0	0	0	0.3	0	0	0	0	0.05

Falls

rolling stock	high speed train									
derailment speed	>15									
derails to cess/adj	cess					adj				
location	open track	in station	tt tunnel	th. station	tunnel app.	open track	in station	tt tunnel	th. station	tunnel app.
FALSE	0.975	1	0.995	1	0.975	0.975	0.95	0.975	0.975	0.975
TRUE	0.025	0	0.005	0	0.025	0.025	0.05	0.025	0.025	0.025

rolling stock	high speed train									
derailment speed	<15									
derails to cess/adj	cess					adj				
location	open track	in station	tt tunnel	th. station	tunnel app.	open track	in station	tt tunnel	th. station	tunnel app.
FALSE	0.9875	1	0.9975	1	0.9875	0.9875	0.9975	0.9975	0.9875	0.9875
TRUE	0.0125	0	0.0025	0	0.0125	0.0125	0.0025	0.0025	0.0125	0.0125

rolling stock	EMU									
derailment speed	>15									
derails to cess/adj	cess					adj				
location	open track	in station	tt tunnel	th. station	tunnel app.	open track	in station	tt tunnel	th. station	tunnel app.
FALSE	0.95	1	0.99	1	0.95	0.95	0.99	0.95	0.95	0.95
TRUE	0.05	0	0.01	0	0.05	0.05	0.01	0.05	0.05	0.05

rolling stock	EMU									
derailment speed	<15									
derails to cess/adj	cess					adj				
location	open track	in station	tt tunnel	th. station	tunnel app.	open track	in station	tt tunnel	th. station	tunnel app.
FALSE	0.975	1	0.995	1	0.975	0.975	0.995	0.995	0.975	0.975
TRUE	0.025	0	0.005	0	0.025	0.025	0.005	0.005	0.025	0.025

Hits

derailment speed	>15									
lineside density	low									
location	open track		in station		twin track tunnel		through station		tunnel approach	
carriages fall	FALSE	TRUE	FALSE	TRUE	FALSE	TRUE	FALSE	TRUE	FALSE	TRUE
FALSE	0.8	0.75	1	1	1	1	1	1	0.8	0.75
TRUE	0.2	0.25	0	0	0	0	0	0	0.2	0.25

derailment speed	>15									
lineside density	low									
location	open track		in station		twin track tunnel		through station		tunnel approach	
carriages fall	FALSE	TRUE	FALSE	TRUE	FALSE	TRUE	FALSE	TRUE	FALSE	TRUE
FALSE	0.95	0.9	1	1	1	1	1	1	0.95	0.9
TRUE	0.05	0.1	0	0	0	0	0	0	0.05	0.1

derailment speed	<15									
lineside density	high									
location	open track		in station		twin track tunnel		through station		tunnel approach	
carriages fall	FALSE	TRUE	FALSE	TRUE	FALSE	TRUE	FALSE	TRUE	FALSE	TRUE
FALSE	0.85	0.8	1	1	1	1	1	1	0.85	0.8
TRUE	0.15	0.2	0	0	0	0	0	0	0.15	0.2

derailment speed	<15									
lineside density	low									
location	open track		in station		twin track tunnel		through station		tunnel approach	
carriages fall	FALSE	TRUE	FALSE	TRUE	FALSE	TRUE	FALSE	TRUE	FALSE	TRUE
FALSE	0.98	0.95	1	1	1	1	1	1	0.98	0.95
TRUE	0.02	0.05	0	0	0	0	0	0	0.02	0.05

Collapse

lineside type	fixed							
crashworthiness	high		low		high		low	
derailment speed	>15	<15	>15	<15	>15	<15	>15	<15
FALSE	0.85	0.95	0.8	0.9	0.98	0.99	0.95	0.98
TRUE	0.15	0.05	0.2	0.1	0.02	0.01	0.05	0.02

Collision

density of traffic	high		low	
direction	cess	adj line	cess	adj line
FALSE	1	0.9	1	0.99
TRUE	0	0.1	0	0.01

Consequence nodes

This section shows the NPTs, and equations used to quantify the hierarchy of nodes used to calculate consequence probabilities shown in Figure B-5.

4 5 6

collapse	FALSE		TRUE	
hits	FALSE	TRUE	FALSE	TRUE
3	1	0	1	0
4	0	1	0	0
5	0	0	0	1

7 8 9

collapse	FALSE		TRUE	
hits	FALSE	TRUE	FALSE	TRUE
6	1	0	1	0
7	0	1	0	0
8	0	0	0	1

11 12 13 14

falls	FALSE		TRUE	
collision	FALSE	TRUE	FALSE	TRUE
9	1	0	0	0
10	0	1	0	0
11	0	0	1	0
12	0	0	0	1

4 5 6 7 8 9

If 'falls' = TRUE then consequence is '789' else consequence is '456'

3 4 5 6 7 8 9

If 'hit tunnel' = TRUE then consequence is '3' else consequence is '456789'

10 11 12 13 14

If 'hit tunnel' = TRUE then consequence is '10' else consequence is '11 12 13 14'

3 - 14

If 'direction' = 'cess' then consequence is '3456789' else consequence is '9 10 11 12 13 14'

2 - 14

If 'clear' = 'true' then consequence is '2' else consequence is '3 -14'

1 – 12

If 'contained' = 'true' then consequence is '1' else consequence is '2 -14'

B.3.4 Model output

In this section we present the model output calculations used to investigate how changing the state of conditions/parameters in the model affected the derailment accident probabilities calculated by the model.

First we present the output calculations for the model calculated with a range of different conditions sets:

	Commuter railway (as outlined in column 1 of Table 4)	Commuter railway with containment fitted	Commuter railway with no curved track	Commuter railway with low traffic density
1	0	0.207595	0	0
2	0.312864	0.241229	0.790348	0.312864
3	0.002433	0.0021901	0.000857	0.002433
4	0.29204	0.229213	0.086682	0.29204
5	0.003041	0.0027369	0.001071	0.003041
6	0.00016	0.000144	0.000056	0.00016
7	0.00244	0.002196	0.000859	0.00244
8	0.0002	0.0001801	0.00007	0.0002
9	0.000011	0.0000095	0.000004	0.000011
10	0.000487	0.000438	0.000171	0.000487
11	0.333711	0.27023	0.103043	0.367083
12	0.037079	0.0300356	0.011449	0.003708
13	0.01398	0.0124309	0.00485	0.015378
14	0.001553	0.0013812	0.000539	0.000155

Table B-2: estimated derailment consequences per derailment for a commuter railway (with a range of different condition sets)

These results are then scaled by the annual probability of occurrence of derailment, calculated in the original study (2.59E-02) on the network to estimate the accident outcome probabilities per year:

	Commuter railway (as outlined in column 1 of Table 4)	Commuter railway with containment fitted	Commuter railway with no curved track	Commuter railway with low traffic density
1	0	0.005376711	0	0
2	0.008103178	0.006247831	0.020470013	0.008103178
3	6.30147E-05	5.67236E-05	2.21963E-05	6.30147E-05
4	0.007563836	0.005936617	0.002245064	0.007563836
5	7.87619E-05	7.08857E-05	2.77389E-05	7.87619E-05
6	0.000004144	3.7296E-06	1.4504E-06	0.000004144
7	0.000063196	5.68764E-05	2.22481E-05	0.000063196
8	0.00000518	4.66459E-06	0.000001813	0.00000518
9	2.849E-07	2.4605E-07	1.036E-07	2.849E-07
10	1.26133E-05	1.13442E-05	4.4289E-06	1.26133E-05
11	0.008643115	0.006998957	0.002668814	0.00950745
12	0.000960346	0.000777922	0.000296529	9.60372E-05
13	0.000362082	0.00032196	0.000125615	0.00039829
14	4.02227E-05	3.57731E-05	1.39601E-05	4.0145E-06

Table B-3: estimated derailment consequences per annum for a commuter railway (with a range of different condition sets)

The graphs that follow show how the probability of occurrence of derailment accidents per year estimated, varies when condition states are revised:

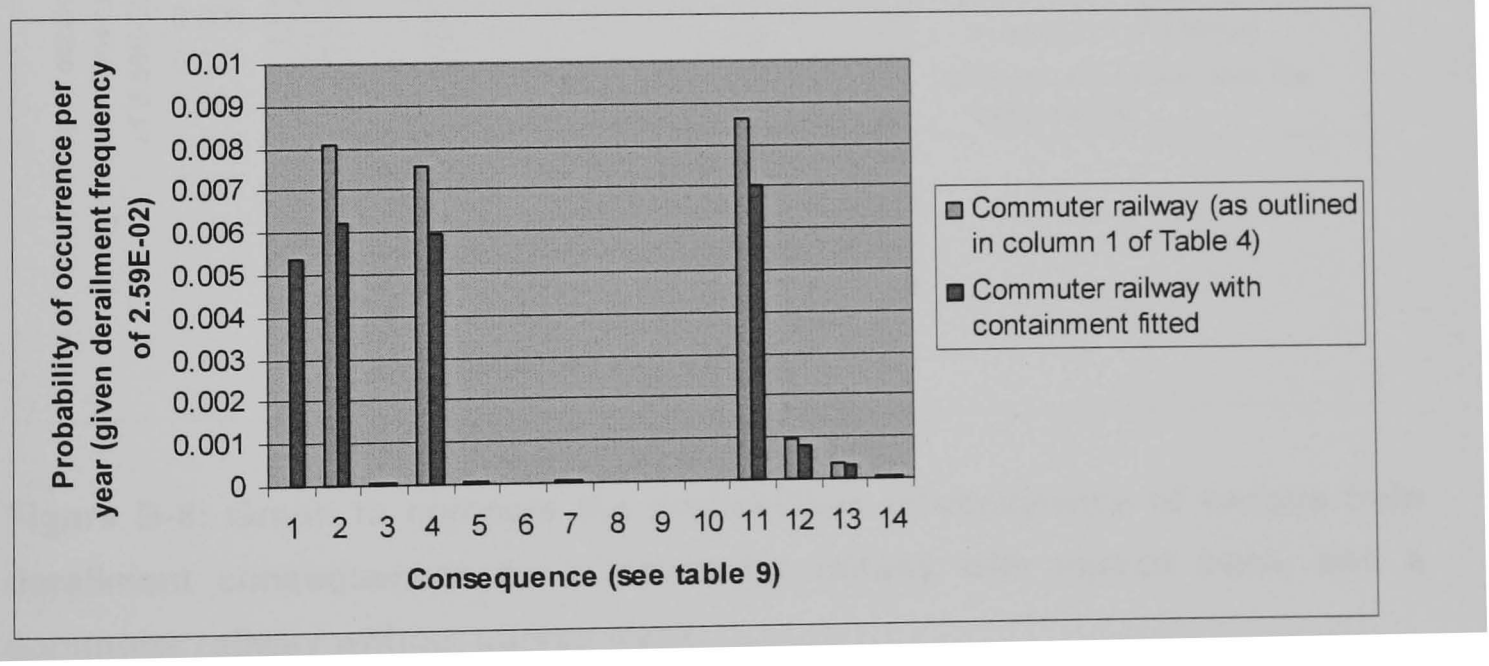


Figure B-6: Graph to compare the probabilities of occurrence of various train derailment consequences for a commuter railway with a containment rail fitted, and a commuter railway without containment rail fitted.

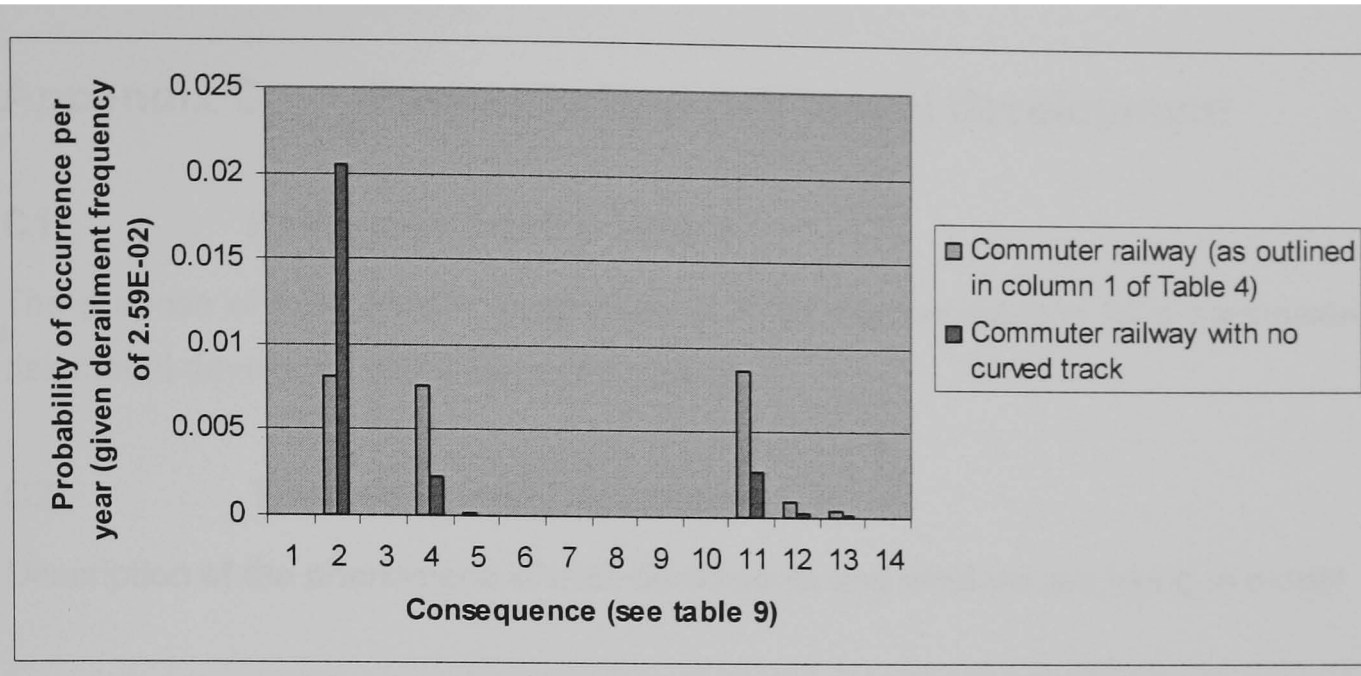


Figure B-7: Graph to compare the probabilities of occurrence of various train derailment consequences for a commuter railway with curved track, and a commuter railway without curved track.

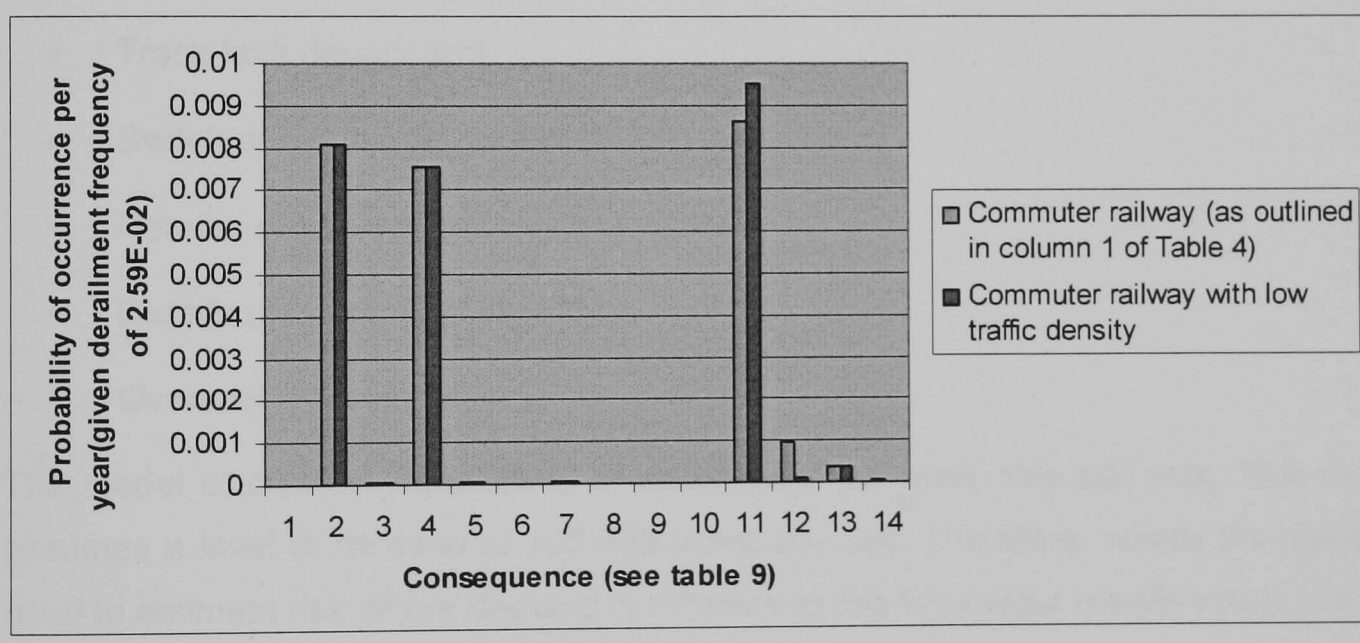


Figure B-8: Graph to compare the probabilities of occurrence of various train derailment consequences for a commuter railway with curved track, and a commuter railway without curved track.

Appendix C Parameterised risk model development

C1 Background and purpose

The purpose of this report is to describe in detail the specification for a parameterised risk model developed using Bayesian Networks.

C2 Train derailment accidents

Description of the phenomena of train derailments and what we are trying to model

C3 Scope of model

The fault tree part of the model represents the causal mechanisms that lead to the occurrence of a derailment. First, we summarise these mechanisms so that the fault tree logic can be understood. In our model, five key types of cause are distinguished:

- Track fault derailments
- Switch and crossing derailments
- Derailments due to rolling stock faults
- Derailments due to obstructions
- Overspeed derailments.

The model calculates probabilities of occurrence per track mile per year. The model assumes a level of demand of 100-299 trains per day. Therefore, where the model is used to estimate risk where demand is different to this the output results would need to be adjusted accordingly.

Track faults

A large number of derailments on GB rail infrastructure occur as a result of track faults of different types. Railway Group Standards ((GC/RT5021) list a large number of faults that should be monitored. We limit our concerns to four types of fault: gauge spreading, track twist, buckled rail and subsidence/landslip.

Gauge spreading is a failure to maintain the correct gauge separation between two rails. When the gauge has spread the passing of a train can force rails back into position, but if this is not possible then derailment will inevitably result. If gauge spread is detected the track must be realigned. Temporary mechanical braces are sometimes used as an intermediate measure, in which case a temporary speed restriction might

be applied. Track twist occurs when the rail becomes twisted such that it is no longer at a 90 degree angle to the track bed. This can lead to a derailment as again rail gauge and wheel separation will be mismatched and the wheels can 'climb' over the rail. A broken rail is a rail that has either a complete fracture through its full cross section or a piece detached entirely from the rail. If such a situation arises, there will be a high risk of derailment for any train passing over that section of track. Subsidence of the ground supporting the track can lead to derailment by altering the gauge spread and height in a variety of ways. Detection of track faults is undertaken by both visual inspection, and the use of dedicated detection equipment. If track faults are detected various control measures might be put in place, from speed restrictions and temporary mechanical fixes to compete closure of the line.

Switch and crossing derailments

A Switch and Crossing (commonly referred to as a set of points) is a track layout that allows rails to be switched to guide a train onto a diverging route or to merge with another route. Derailment is possible when rails are not correctly locked into position, making it possible for wheels to come off of the rail. Derailment risk is particularly high where there are facing points, which lead to diverging routes, as was the case at the location of the Potters Bar derailment. S&C errors can be caused by poor maintenance, such as misaligned rails, or failure to properly tighten screws or locking nuts following maintenance. Because of the high risk associated with S&C errors any identified faults would tend to be addressed as a matter of urgency.

Derailments due to rolling stock faults

The model includes four types of rolling stock fault that could lead to derailment:

- Brake failure
- Axle box failure
- Wheel flats
- Suspension/bogie failure

Brake failure can lead to trains over speeding and hence derailments occurring due to large forces between the wheel and rail, particularly at tight corners. The key axle box failure is a 'hot axle box' where the axle bearing overheats because of poor lubrication. This can result in the axle fracturing. Hot axle box detectors, fixed at lineside, are used to detect them. A wheel flat is a flat spot on the rolling surface of the wheel caused by the wheel sliding on the rail. This can result in large dynamic forces between the wheel

and rail which can result in the wheel fracturing or riding over the rail. Suspension failures have the potential to lead to the wheel jumping from the rail where vertical movement of the train is not sufficiently damped.

Derailments due to obstructions

Collision with significant objects which obstruct the path of the train can obviously result in train derailment. Even smaller objects, if placed in certain locations, can greatly increase the risk of derailment. In our model we include obstruction by engineering material, debris from lineside overbridge, objects from trains, landslip/fallen trees, objects placed by vandals, and the presence of large animals.

Overspeed derailments

Overspeed derailments occur when a train driver fails to obey a speed limit and the train derails because the wheel-rail forces exceed their design limits. We classify over speed derailments as derailments of this type where the driver causes the train to overspeed, rather than overspeed due to any mechanical fault to the train, such as brake failure (which is described in 1.3.3).

General

The resulting model calculates the relative probabilities of occurrence of a range of possible outcomes following derailment due to these causes. The consequences of a derailment accident and the condition states that impact upon those consequences are not explicitly modelled. The events and condition states that are modelled are described in sections 3, 2 and 3.

This document should be read in conjunction with files:

- Derailment model - NPTs v1.0.doc
- Parameterised derailment model v1.0.hkb/.net

C4 Fault tree structure and events

In this section of the Appendix C, the structure and meaning of the fault tree part of the model is shown and described.

C.4.1 Logical fault tree structure

The fault tree modelling all possible derailment causes is shown below.in the following diagrams:

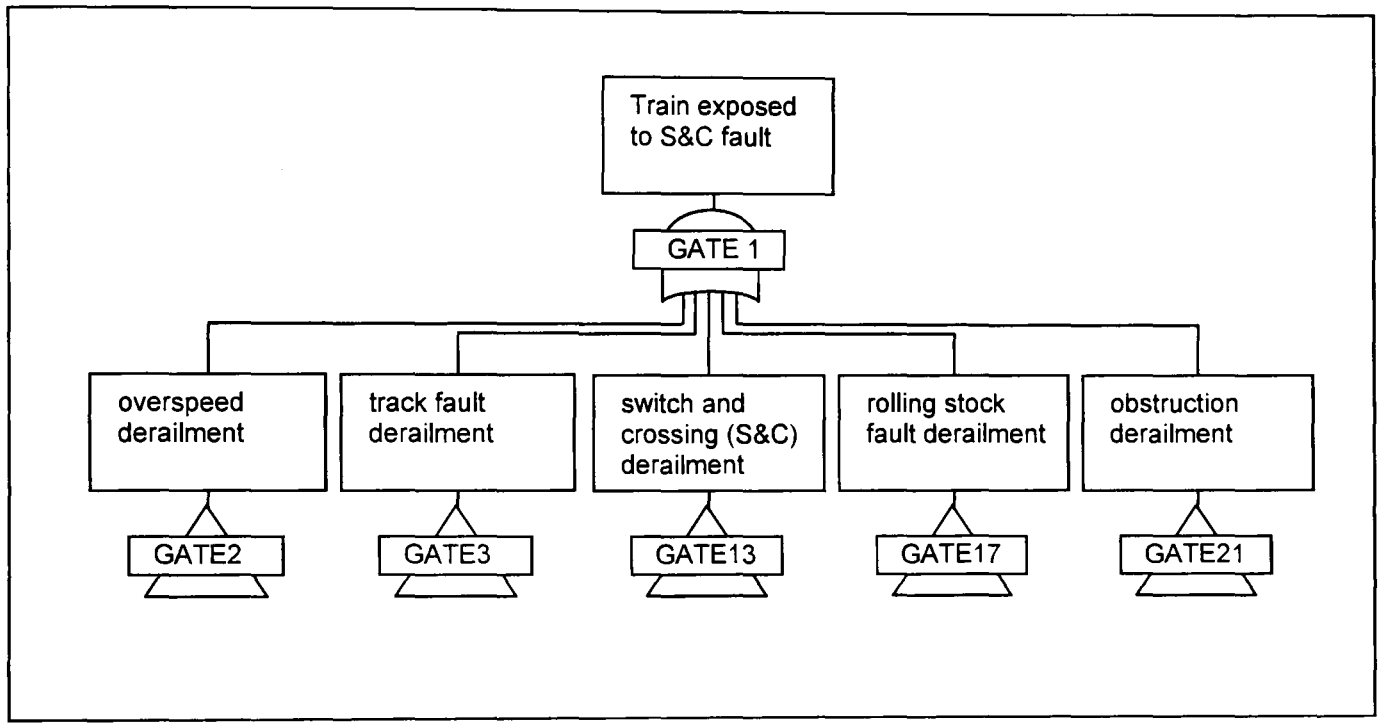


Figure C-1: Top event gate of derailment fault tree fragment

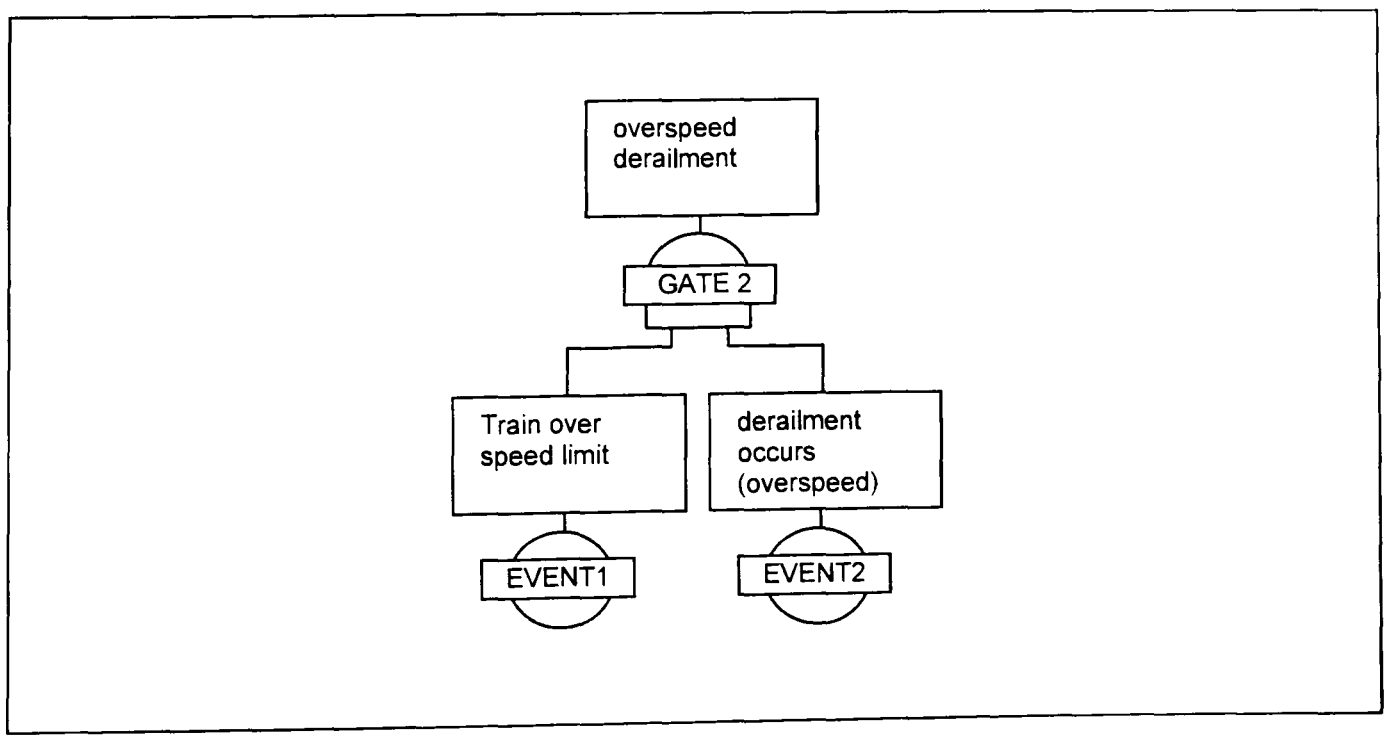


Figure C-2: Overspeed derailment fault tree fragment

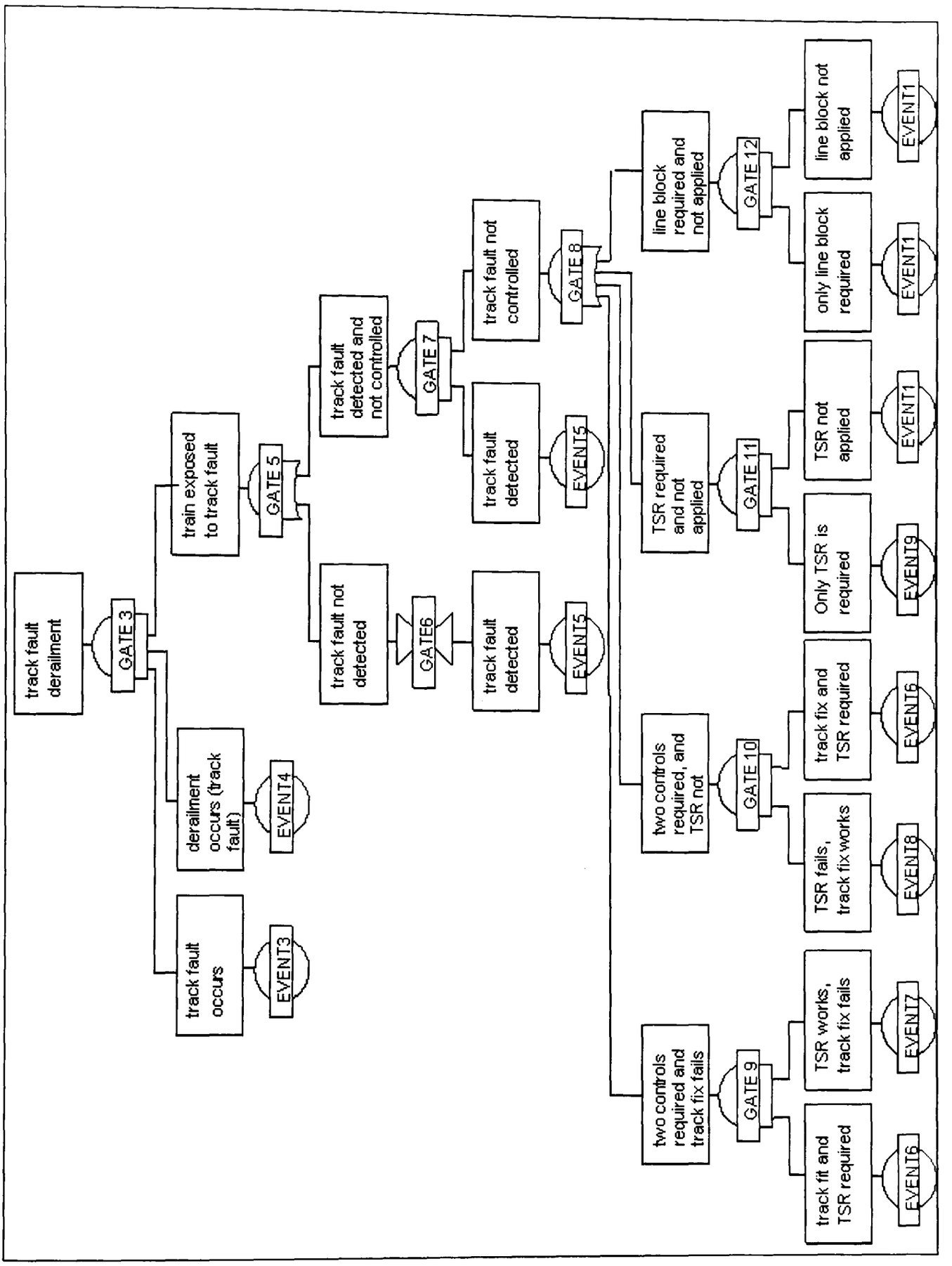


Figure C-3: Track fault derailment fault tree fragment

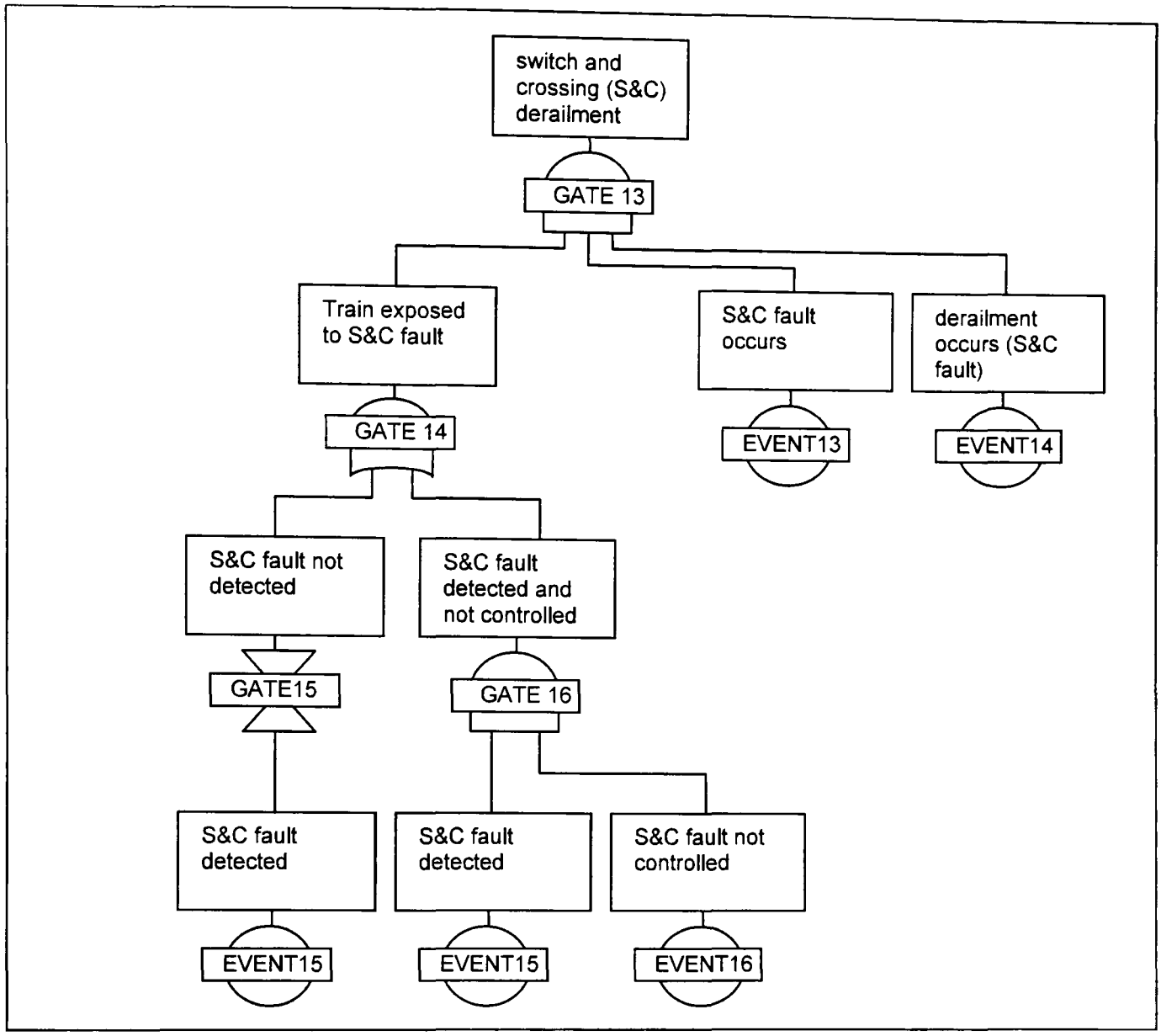


Figure C-4: Switch and crossing derailment fault tree fragment

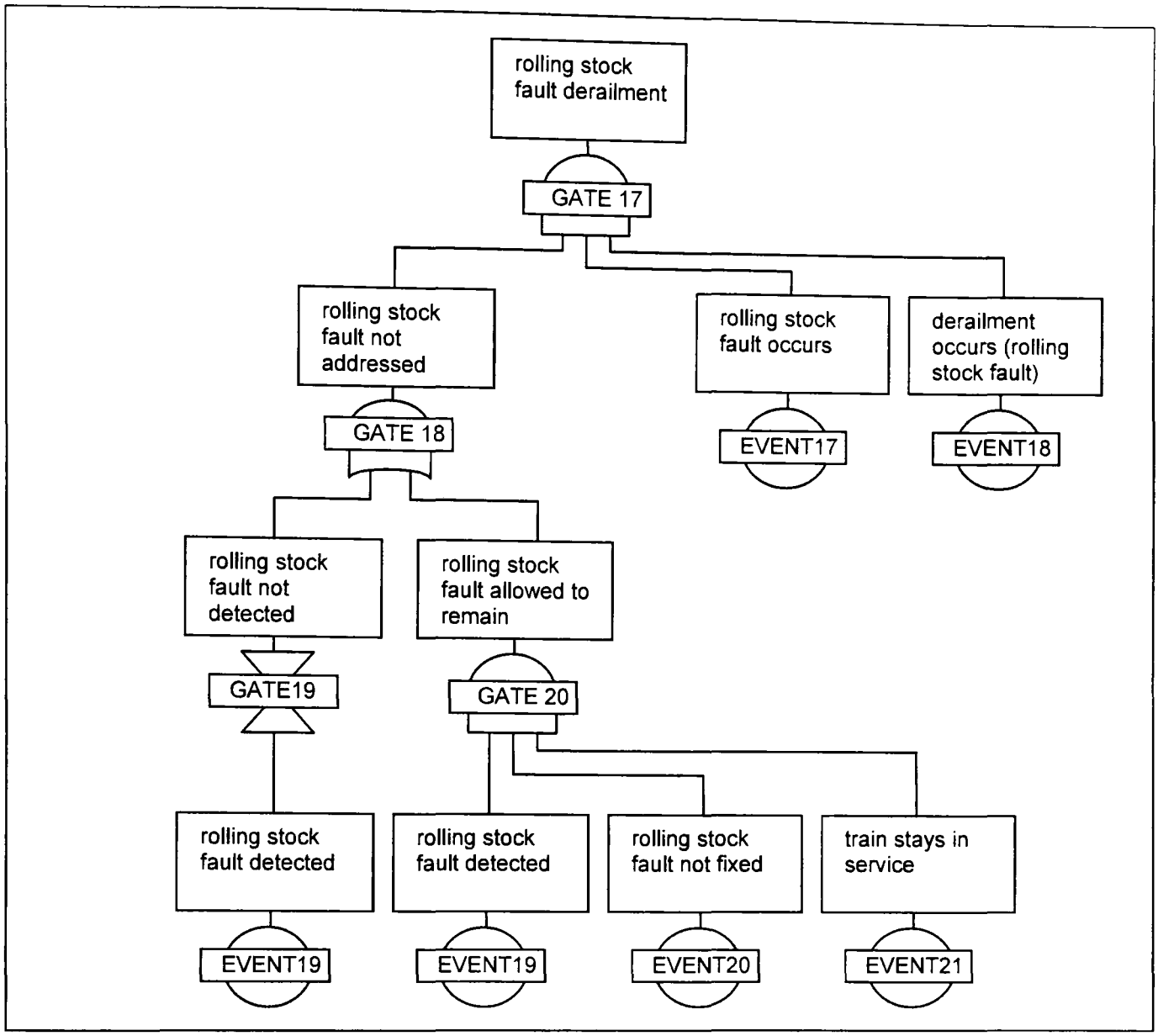


Figure C-5: Rolling stock derailment fault tree fragment

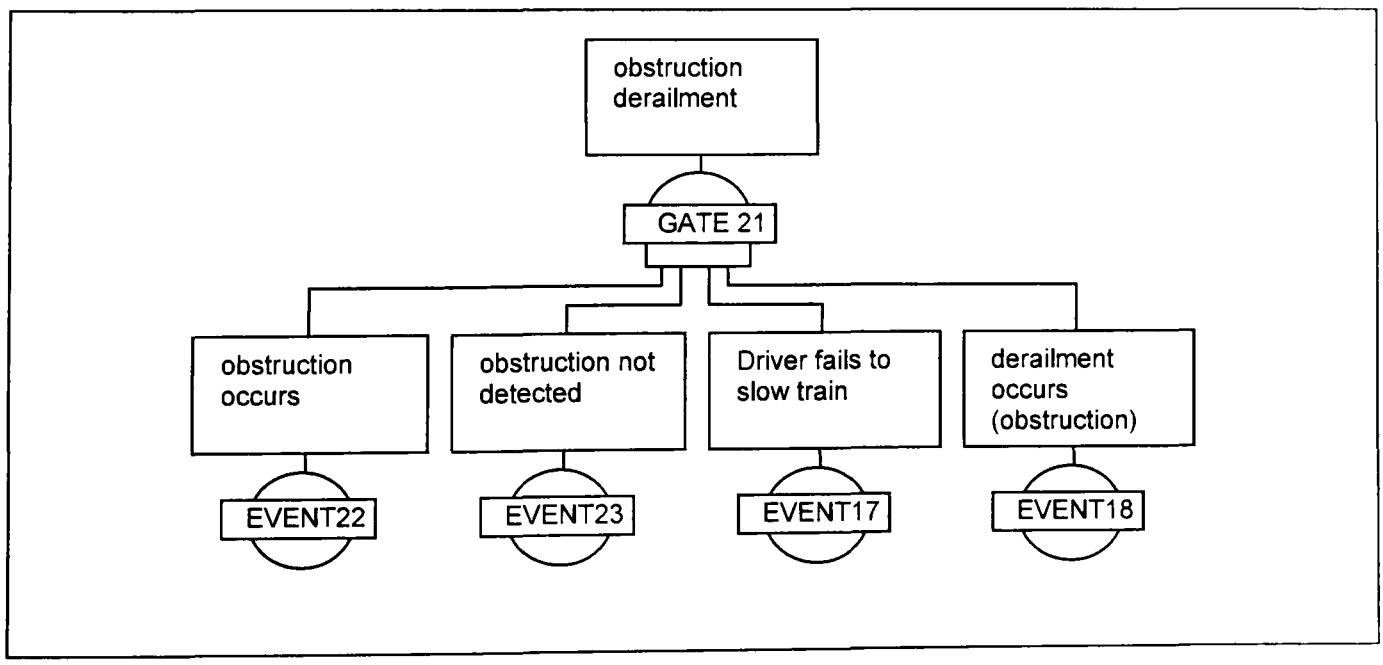


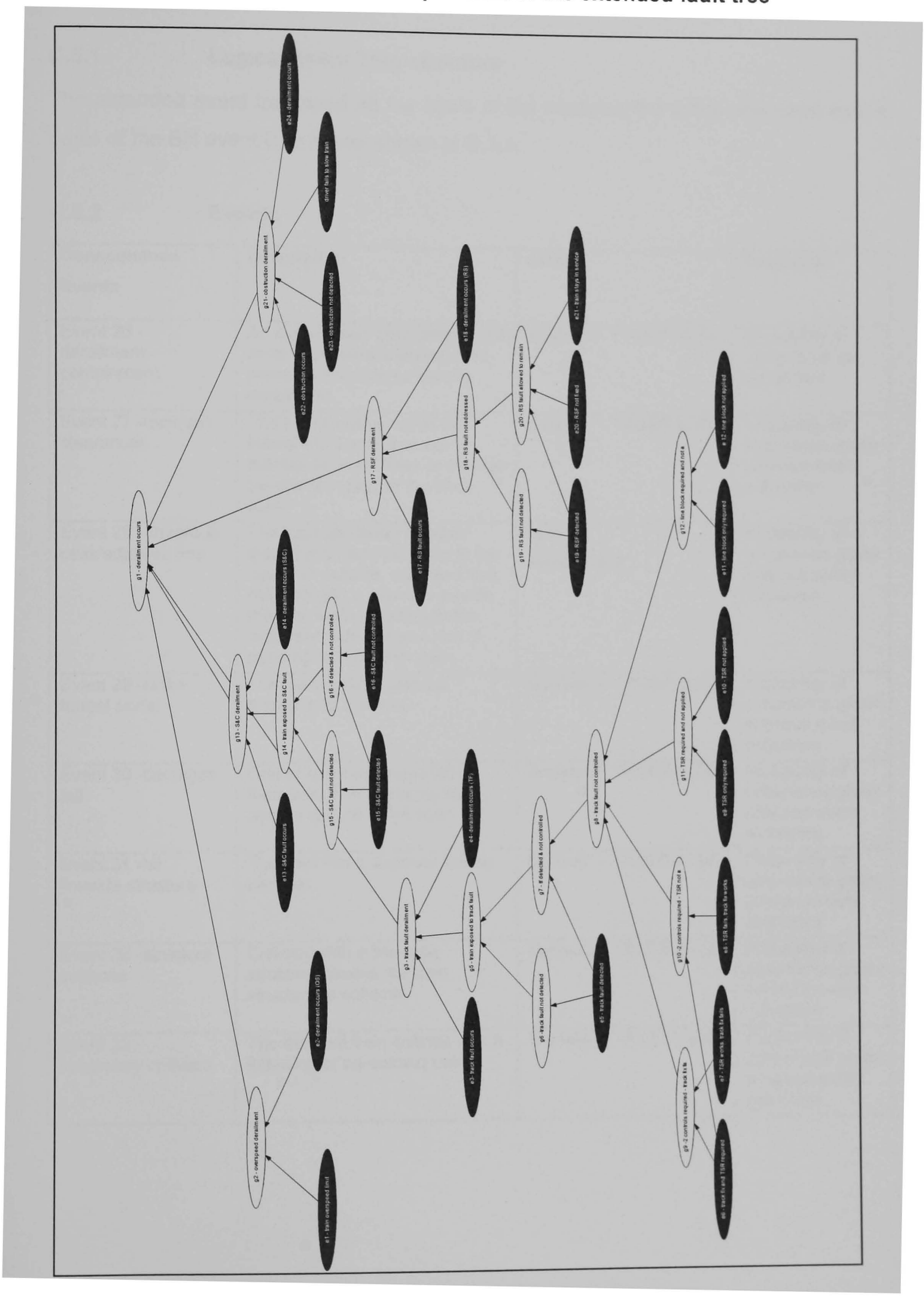
Figure C-6: Obstruction derailment fault tree fragment

C.4.2 Fault Tree probabilities

Base Event	Description	States	Comment
Event 1 – train over speed limit	A train on a given mile section of track passes at above the speed limit.	Boolean – TRUE/ FALSE	Event occurrence per track mile per year (frequency)
Event 2 – derailment occurs (overspeed)	A train derailment occurs due to the train passing a mile section of track at above the speed limit	Boolean – TRUE/ FALSE	Probability given event 1 is true. (unavailability)
Event 3 - track fault occurs	The occurrence of any track fault. This is an absolute probability of occurrence per track mile. (The occurrence of different sorts of track fault is modelled with a separate node).	Boolean – TRUE/ FALSE	Event occurrence per track mile per year (frequency)
Event 4 derailment occurs (track fault)	A train derailment occurs due to the presence of a track fault.	Boolean – TRUE/ FALSE	Probability given event 3 and gate 5 are true. (unavailability)
Event 5 – track fault detected	The track fault is detected by routine inspections.	Boolean – TRUE/ FALSE	Probability given event 3 is true. (unavailability)
Event 6 – track fix and TSR required	Following the detection of a track fault, a track fix (gauge restraint or rail clamping) and TSR are required to mitigate risk.	Boolean – TRUE/ FALSE	Probability given event 3 is true. (unavailability)
Event 7 - TSR works, track fix fails,	The TSR is correctly applied and the track fix is not correctly applied, given that a track fault has occurred and both controls are the required response.	Boolean – TRUE/ FALSE	Probability given event 3 and event 5 are true. (unavailability)
Event 8 – TSR fails, track fix works,	The Track fix is correctly applied and the TSR is not correctly applied, given that a track fault has occurred and both controls are the required response.	Boolean – TRUE/ FALSE	Probability given event 3 and event 5 are true. (unavailability)
Event 9 – TSR only required	Following the detection of a track fault, a TSR is required to mitigate risk.	Boolean – TRUE/ FALSE	Probability given event 3 and event 5 are true. (unavailability)
Event 10 – TSR not applied	A TSR is not imposed or is not effective when a track fault has occurred which requires only a TSR as a control.	Boolean – TRUE/ FALSE	Probability given event 3 and event 5 are true. (unavailability)
Event 11 – line block only required.	Following the detection of a track fault, a line block is required to mitigate risk.	Boolean – TRUE/ FALSE	Probability given event 3 and event 5 are true. (unavailability)
Event 12- line block not applied	A line block is not imposed when a track fault has occurred which requires a line block as a control.	Boolean – TRUE/ FALSE	Probability given event 3 and event 5 are true. (unavailability)

Base Event	Description	States	Comment
Event 13 – S&C fault occurs	A fault occurs on a switch and crossing system.	Boolean – TRUE/ FALSE	Event occurrence per track mile per year (frequency)
Event 14 – derailment occurs (switch and crossing fault)	A train derailment occurs due to the presence of a switch and crossing fault.	Boolean – TRUE/ FALSE	Probability given event 13 and gate 14 are true. (unavailability)
Event 15 – S&C fault detected	The S&C fault is detected by routine inspections.	Boolean – TRUE/ FALSE	Probability given event 13 is true. (unavailability)
Event 16 – S&C fault not controlled	An S&C fault which has been detected is not controlled.	Boolean – TRUE/ FALSE	Probability given event 13 and event 15 are true. (unavailability)
Event 17- rolling stock fault occurs	A rolling stock fault occurs as a train travels over a particular mile of track.	Boolean – TRUE/ FALSE	Event occurrence per track mile per year (frequency)
Event 18 – derailment occurs (rolling stock fault)	A derailment occurs due to a rolling stock fault.	Boolean – TRUE/ FALSE	Probability given event 17 and gate 18 are true. (unavailability)
Event 19 – rolling stock fault detected	A rolling stock fault is detected.	Boolean – TRUE/ FALSE	Probability given event 17 is true. (unavailability)
Event 20 – rolling stock fault not fixed	Rolling stock fault not fixed.	Boolean – TRUE/ FALSE	Probability given event 17 and event 19 are true. (unavailability).
Event 21 – train stays in service	A train which should be removed from service, following the detection of a rolling stock fault, stays in service.	Boolean – TRUE/ FALSE	Probability given event 17, event 19 and event 20 are true. (unavailability) (assumes that the RSF was detected)
Event 22 – obstruction occurs	The track is blocked by an obstruction of some type.	Boolean – TRUE/ FALSE	Event occurrence per track mile per year (frequency)
Event 23 – obstruction not detected	The obstruction is not detected or noticed prior to the arrival of a train.	Boolean – TRUE/ FALSE	Probability given event 22 is true. (unavailability)
Event 24 – driver fails to slow train	The driver, having seen the obstruction, fails to slow the track down sufficiently to ensure that a derailment does not occur.	Boolean – TRUE/ FALSE	Probability given events 22 and 23 are true (unavailability)
Event 25 – derailment occurs (obstruction)	A train derailment occurs due to the presence of an obstruction.	Boolean – TRUE/ FALSE	Probability given events 22, 23 and 24 are true. (unavailability)

C.4.3 Bayesian Network equivalent of the extended fault tree



C5 Event tree events

C.5.1 Logical Event Tree structure

The extended event tree used as the basis of the model is the same one used as the basis of the BN event tree model shown in B.3.1.

C.5.2 Events

Consequence Events	Description	States	Comment
Event 26 - derailment containment	An extra raised 'containment' rail limits movement sideways and prevents the occurrence of a derailment.	Boolean – TRUE/FALSE	Probability of occurrence per derailment.
Event 27 -maintain clearances	The train remains within the lateral limits and does not overlap adjacent lines or obtrude beyond the edge of the track area.	Boolean – TRUE/FALSE	Probability of occurrence given previous event outcomes.
Event 28 - derails to cess/adjacent line	The train can derail to either side of the track: derailing to the 'cess', or outside, may lead to a collision with a structure beside the line, while derailing to the 'adjacent' side brings a risk of colliding with another train.	cess adjacent line	Probability of occurrence given previous event outcomes.
Event 29 -strike tunnel portal	The train collides with the entrance to a tunnel.	Boolean – TRUE/FALSE	Probability of occurrence given previous event outcomes.
Event 30 -carriages fall	One or more carriages fall on their side. The carriages may remain upright or fall over.	Boolean – TRUE/FALSE	Probability of occurrence given previous event outcomes.
Event 31 -hit lineside structure	The train hits a structure beside the line.	Boolean – TRUE/FALSE	Probability of occurrence given previous event outcomes.
Event 32 -structure collapse	Collision with a line-side structure causes the train structure to collapse.	Boolean – TRUE/FALSE	Probability of occurrence given previous event outcomes.
Event 33 - secondary collision	The derailed train collides with a following or on-coming train.	Boolean – TRUE/FALSE	Probability of occurrence given previous event outcomes.

C.5.3 Conditions

Track conditions

Attribute	Description	States	Comment
Containment fitted	Whether or not a containment rail is fitted to decrease the probability of a derailment occurring.	Boolean – TRUE/FALSE	
Track curvature	The degree of curvature on the track.	Very high (200m radius) High (700m radius) Medium (1200m radius) Low/none (>1500m radius)	
Train speed	The speed that the train is travelling at (miles per hour).	110-125 80-109 40-79 ≤39	
Number of tracks	The number of adjacent tracks in the area where the derailment occurs.	1 2 4	
Track inspection intervals	The interval of time between scheduled inspections.	1wk 2 wks 4 wks	
Track type	The type of track.	Plain Line S&C	
Rolling stock inspection interval	The time interval between scheduled rolling stock inspections.	1wk 2 wks 4 wks	

Location conditions

Attribute	Description	States	Comment
Lineside object density	The number of lineside objects adjacent to the track in the area where the derailment occurs.	high low	
Lineside object type	The type of lineside object adjacent to the track in the area where the derailment occurs. The objects are characterised by considering how much of an obstacle they will present to the movement of a train. Anchored equipment is something that could be knocked from the ground, like a signal post. Fixed equipment is something like a concrete structure that would significantly deform the derailed train.	fixed anchored	
Location of track	The location in which any given mile of track is located.	in tunnel on tunnel approach outside rural outside urban in station	

Performance conditions

Attribute	Description	States	Comment
Competence of infrastructure maintainer	A qualitative judgement of the overall competence of IM maintenance on any given mile of the infrastructure.	High Medium Low	Assumed values – would need to be determined by a programme of monitoring
Competence of rolling stock maintainer	A qualitative judgement of the overall competence of rolling stock maintenance on any given mile of the infrastructure.	High Medium Low	Assumed values – would need to be determined by a programme of monitoring
Driver experience	A qualitative judgement of the experience of drivers on any given mile of the infrastructure.	High Medium Low	Assumed values – would need to be determined by a programme of monitoring

C.5.4 Faults

Rolling stock faults

Attribute	Description	States	Comment
Rolling stock fault type	Each possible fault type on the rolling stock per track mile per year.	brake failures axle/axle box failure wheel faults/failure suspension/bogie failure	
Rolling stock fault severity	Each possible severity of rolling stock fault.	high medium low	

Track faults

Attribute	Description	States	Comment
Track fault type	Each possible track fault type on the track.	gauge spreading track twist broken rail buckled rail subsidence/landslip	-
Track fault severity	The severity of track fault/s occurring on the network.	high medium low	-
S&C fault severity	The severity of S&C fault/s occurring on the network.	high medium low	-
Type of obstruction	Each possible obstruction on the track.	engineering material debris from lineside/overbridge objects from trains landslip/fallen trees from vandals large animals	-

C6 Correlation charts

In all tables that follow, mid-grey shaded boxes indicate that the variable in the row is a 'child' of the variable indicated in the relevant column. A light-grey shaded box indicates that the variable in the row is a 'parent' of the variable indicated in the relevant column. In the conditions-conditions correlation chart only, the child relationships are shown (as no further information would be provided by highlighting the inverse parent relationships between conditions).

C.6.1 Fault tree base events and conditions

Event	Containment fitted?	Track curvature	Train speed	Number of tracks	Track inspect. intervals	Track type	Lineside object density	Lineside object type	Location of track	Rolling stock fault type	Rolling stock fault sev.	R.Stock inspect. interv	Track fault type	Track fault severity	S&C fault severity	Type of obstruction	Competence of infra-structure maintainer	Competence of rolling stock maintainer	Driver experience
1																			
2																			
3																			
4																			
5																			
6																			
7																			
8																			
9																			
10																			
11																			
12																			
13																			
14																			
15																			
16																			
17																			
18																			
19																			
20																			
21																			
22																			
23																			
24																			
25																			

C.6.2 Event tree events and conditions

Event	26	27	28	29	30	31	32	33
Containment fitted?								
Track curvature								
Train speed								
Number of tracks								
Track inspect. intervals								
Track type								
Lineside object density								
Lineside object type								
Location of track								
Rolling stock fault type								
Rolling stock fault sev.								
R.Stock inspect. interv								
Track fault type								
Track fault severity								
S&C fault severity								
Type of obstruction								
Competence of infra-structure maintainer								
Competence of rolling stock maintainer								
Driver experience								

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	Conditions
1	■																			1 - Containment fitted
2		■																		2 - Track curvature
3			■																	3 - Train speed
4				■																4 - Number of tracks
5					■															5 - Track inspect. intervals
6						■														6 - Track type
7							■													7 - Lineside object density
8								■												8 - Lineside object type
9									■											9 - Location of track
10										■										10 - Rolling stock fault type
11											■									11 - Rolling stock fault sev.
12												■								12 - R.Stock inspect. interv
13													■							13 - Track fault type
14														■						14 - Track fault severity
15															■					15 - S&C fault severity
16																■				16 - Type of obstruction
17																	■			17 - Competence of infra-structure maintainer
18																		■		18 - Competence of rolling stock maintainer
19	■																			19 - Driver experience

C7 Translation into a BN

The Bayesian Network showing all fault and event tree events is shown in C.4.3.

C8 Quantification of the model

The NPTs in the Bayesian Network are quantified using a combination of available data and expert judgement.

The primary data sources were:

- The RSSB Annual Safety Performance Report, 2006
- Network Rail Performance Plan, 2006
- The RSSB report, Derailment Risk Model (Track Faults) Phase 1 report, D4145/003/01
- Railway Group Standard GC/RT5021
- Thameslink 2000 derailment report TL/MPD/TL2/SAF/026

Elicitation of probabilities was undertaken with the support of David Harris, and Peter Dray, of Sotera Risk Solutions at a meeting held on 12 June 2007

A complete set of NPTs used to quantify the BN model was developed in an excel file. Sections C.8.1 to C.8.3 provide three examples of NPTs and supporting information taken from this file. In the NPT tables shown, entries are shown in **bold** where they have been derived from some specific evidence, assertion by a railway professional or technical report. Appropriate references to source information are given. The tables are then completed by using expert judgement to extrapolate this known data according to the perceived relationship between the occurrence of events and the states of the relevant conditions (indicated in each event NPT).

The data is not intended to be rigorous and complete, and the resulting model is not intended for use to support real risk assessment and risk based judgement. Instead the data is intended to be indicative, and to allow the author to fully investigate the possible uses of a Bayesian Network model of this type.

C.8.1 Event 1: train overspeed

driver performance	high			
train speed	110-125	80-109	40-79	<=39
false	1	1	1	1
true	0	0	0	0

driver performance	medium			
train speed	110-125	80-109	40-79	<=39
false	1	0.999999	0.999998	0.999996
true	0	0.000001	0.000002	0.000004

driver performance	low			
train speed	110-125	80-109	40-79	<=39
false	1	0.999996	0.999992	0.999984
true	0	0.000004	0.000008	0.000016

Supporting evidence

The numbers inserted in this NPT are logically self-evident and are derived from the relationship between the track speed limit at any given location and the train speed. Probability estimates are based on estimated event occurrence rates per track mile per year, and are based on a density of service in the area where the derailment has occurred of 100-299 trains per day.

C.8.2 Event 2: derailment occurs due to a train overspeed

train speed	110-125			
track curvature	v high (200m)	high (700m)	medium 1200m	low/none (>1500m)
false	0.9928	0.9964	0.9982	0.9991
true	0.0072	0.0036	0.0018	0.0009

train speed	80-109			
track curvature	v high (200m)	high (700m)	medium 1200m	low/none (>1500m)
false	0.9964	0.9982	**0.9991**	1.000
true	0.0036	0.0018	**0.0009**	0.00045

train speed	40-79			
track curvature	v high (200m)	high (700m)	medium 1200m	low/none (>1500m)
false	0.9982	0.9991	0.99955	0.999775
true	0.0018	0.0009	0.00045	0.000225

train speed	<=39			
track curvature	v high (200m)	high (700m)	medium 1200m	low/none (>1500m)
false	0.9991	0.99955	0.999775	0.9998875
true	0.0009	0.00045	0.000225	0.0001125

Supporting evidence

Meeting with Dave Harris and Peter Dray, 12th June 2007:

Irish Rail risk model: The probability of a derailment occurring following an overspeed through a speed restriction is 9E-04. This figure is for a passenger train.

It was assumed that the figure represents that probability for a train travelling at 80-109mph on with medium track curvature. It is assumed that a derailment on track with low curvature is half as likely as a derailment on track with medium curvature.

It was assumed that a derailment on track with medium curvature is half as likely as a derailment on track with high curvature.

It was assumed that a derailment on track with high curvature is half as likely as a derailment on track with very high curvature.

It was assumed that a derailment due to over speed when travelling at 40-79mph is twice as likely as when travelling at <=39mph

It was assumed that a derailment due to over speed when travelling at 80-109mph is twice as likely as when travelling at 40-79mph

It was assumed that a derailment occurring due to over speed when travelling legitimately at 110-125mph is five times as likely as when travelling at 80-109mph

It was assumed that derailment due purely to overspeed is not possible when travelling at less than 39mph on straight track.

C.8.3 Event 3- track fault occurs

false	**0.56997**
true	**0.43003**

Supporting evidence

Track fault annual totals derived from the 2006 Annual Safety Performance Report (ASPR), page 123.

Broken rails 226 per annum

Buckled rails 85 per annum

Landslips/subsidence 12 per annum

Network Rail Performance Plan 2006:

Route miles 16,115

Types of fault	Per mile average
Broken rails	0.01402
Buckled rails	0.00527
Subsidence incidents	0.00074
Level 2 exceedences due to gauge spreading (ASPR page 237):	0.01

Level 2 exceedences due to track twist (ASPR, page 237):	0.4
Total	0.43003

The probability total is an absolute probability of occurrence per track mile. Probability estimates are based on a density of service in the area where the derailment has occurred of between 100-299 trains per day.

C9 Validation of the model

C.9.1 Typical location conditions

In order to validate the model, output calculation results calculated with a given set of condition states were compared against output results for the fault and event tree equivalents. Table C-1 (below) shows the set of conditions used for a fairly typical location on the GB rail network.

Conditions	Typical mile section of UK rail network
containment fitted	no
track curvature	low/none
train speed	40-79
number of tracks	2
track inspection intervals	2 week
track type	switch and crossing
lineside object density	low
lineside object type	anchored
location of track	outside rural
rolling stock inspection interval	2 weeks
driver experience	medium
competence of rolling stock maintainer	medium
competence of infrastructure maintainer	medium
track fault type	distribution – no evidence entered
track fault severity	distribution
S&C fault severity	distribution
type of obstruction	distribution
rolling stock fault type	distribution
rolling stock fault severity	distribution

Table C-1: Conditions relating to a typical location on the GB rail network.

C.9.2 Validation of event tree logic

The diagram below shows the event tree representing the event sequence when the set of conditions shown in Table C-1 exist.

The frequencies of occurrence of each of the 14 possible outcomes given the occurrence of a derailment were calculated in a spread sheet and are shown in Figure C-7.

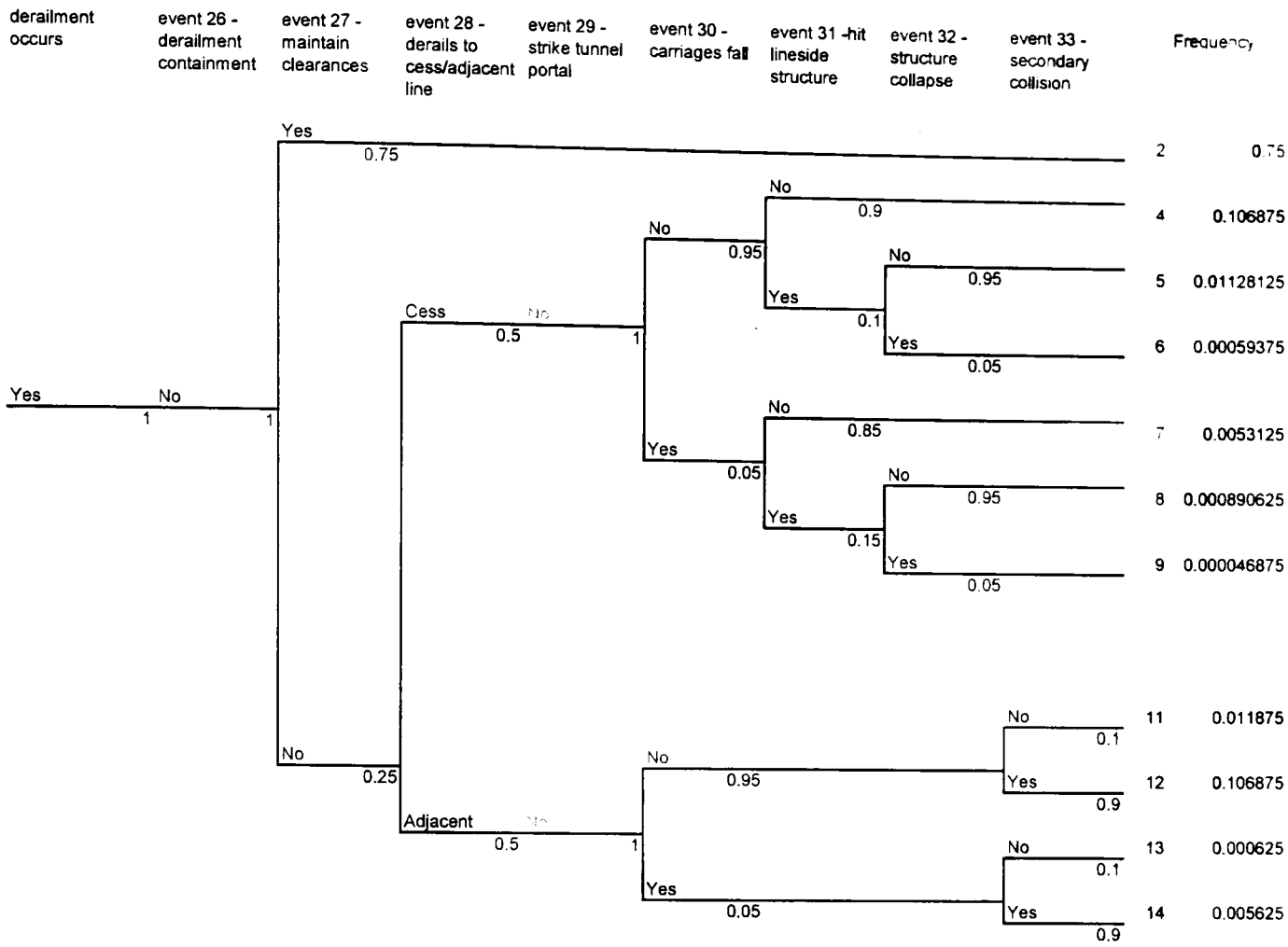


Figure C-7: event tree representing the probability of a range of derailment outcomes in a location where the conditions in Table C-1 are valid.

The conditions shown in Table C-1 were then entered into the Bayesian Network model. In addition to this the event derailment occurs, was set to 'true' to ensure that a direct comparison could be made of the results of each model.

The BN probabilities were then updated and, as can be seen by comparing the results shown in Figure C-7 with those in Figure C-8, the same output probabilities were calculated.

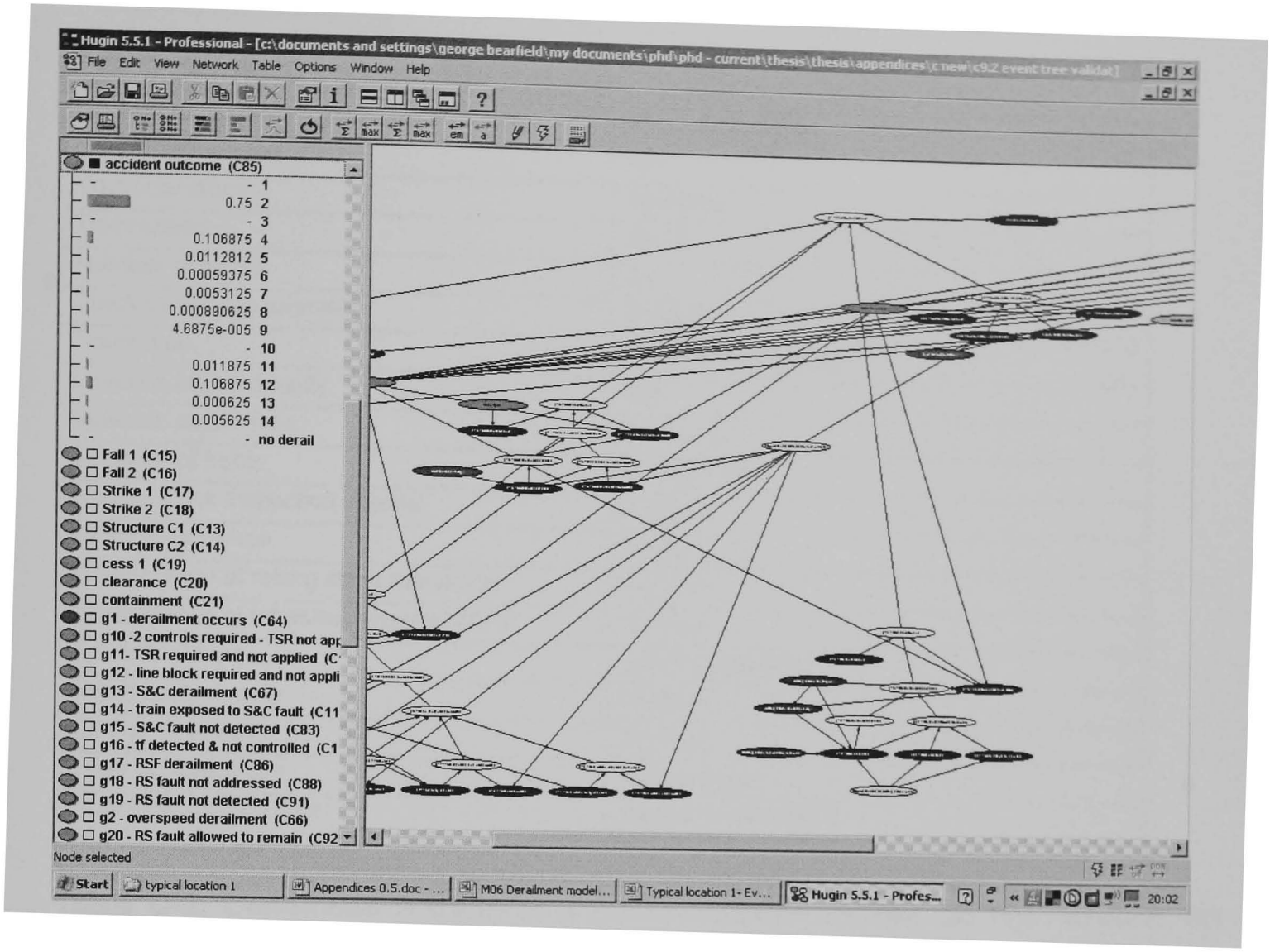


Figure C-8: Screen shot showing the derailment outcome probabilities calculated using the BN model, with the condition states of Table C-1 entered

A selection of different condition sets were checked against the model is a similar way, in order to provide confidence that the event tree logic had been correctly and completely captured in the BN model.

C.9.3 Validation of fault tree logic

The BN logic can represent a wide range of different fault trees. In order to compare the output of the BN fault tree with the output of an actual fault tree it is necessary to enter evidence into the BN so that it represents a particular scenario, which can also be built as a fault tree. The fault condition nodes, whose possible states are modelled as distributions for general use (see **Error! Reference source not found.**) must also be set to a particular state.

This process was followed for a range of different scenarios (and hence fault trees) in order to provide confidence that the fault tree logic had been correctly and completely captured in the BN model. 3 scenarios were considered, and these were selected to fully exercise the track fault logic, which is the most complicated section of the fault tree.

Scenario 1

Condition node	Condition state
Containment fitted	no
Track curvature	low/none
Train speed	40-79
Number of tracks	2
Track inspection intervals	2 weeks
Track type	switch and crossing
Lineside object density	low
Lineside object type	anchored
Location of track	outside rural
Rolling stock inspection interval	2 weeks
Driver experience	medium
Competence of rolling stock maintainer	medium
Competence of infrastructure maintainer	medium
Track fault type	gauge spreading
Track fault severity	medium
S&C fault severity	medium
Type of obstruction	from vandals
Rolling stock fault type	axle/axle box failure
Rolling stock fault severity	high

Table C-2: Conditions relating to a typical location on the GB rail network, for use in the validation of the output of the fault tree section of the BN

The fault tree base event probabilities calculated by the BN when entering the evidence in Table C-2 were:

Event 1: 2.0 e^{-06}
Event 2: 2.41301 e^{-06}
Event 3: 0.43003
Event 4: 5.0 e^{-06}
Event 5: 0.9996
Event 6: 1
Event 7: 0.000999
Event 8: 0.000699
Event 9: 0
Event 10: 0.0007
Event 11: 0
Event 12: 1.0 e^{-06}
Event 13: 0.0006
Event 14: 0.037
Event 15: 0.998
Event 16: 1.0 e^{-06}
Event 17: 0.07179
Event 18: 0.001014
Event 19: 0.999988
Event 20: 1.0 e^{-06}
Event 21: 0.5
Event 22: 0.1739
Event 23: 0.0001
Event 24: 0.1
Event 25: 0.00785

Both the BN (bn fault tree validation 1.hkb) and the fault tree (bn fault tree validation 1.psa) calculated a top event probability, for gate 1, of 2.413e-08.

Scenario 2

Condition node	Condition state
Containment fitted	no
Track curvature	low/none
Train speed	80-109
Number of tracks	4
Track inspection intervals	1 weeks
Track type	plain line
Lineside object density	high
Lineside object type	fixed
Location of track	outside rural
Rolling stock inspection interval	2 weeks
Driver experience	low
Competence of rolling stock maintainer	low
Competence of infrastructure maintainer	low
Track fault type	track twist
Track fault severity	medium
S&C fault severity	-
Type of obstruction	landslip/fallen trees
Rolling stock fault type	axle/axle box failure
Rolling stock fault severity	high

Table C-3: Conditions relating to a typical location on the GB rail network, for use in the validation of the output of the fault tree section of the BN

The fault tree base event probabilities calculated by the BN when entering the evidence in Table C-3 were:

Event 1: 4.0 e^{-06}
Event 2: 4.5 e^{-05}
Event 3: 0.43003
Event 4: 0.000294
Event 5: 0.9996
Event 6: 0
Event 7: 0.0001997
Event 8: 0.001397
Event 9: 1
Event 10: 0.00035
Event 11: 0
Event 12: 2.0 e^{-06}
Event 13: 0
Event 14: 0.115625
Event 15: 0.999641
Event 16: 2.0 e^{-06}
Event 17: 0.07179
Event 18: 0.005071
Event 19: 0.999975
Event 20: 2.0 e^{-06}
Event 21: 1
Event 22: 0.1739
Event 23: 0.00015
Event 24: 0.64
Event 25: 0.00294

Both the BN (bn fault tree validation 2.hkb) and the fault tree (bn fault tree validation 2.psa) calculated a top event probability, for gate 1, of 5.956e-07.

Scenario 3

Condition node	***Condition state***
containment fitted	false
track curvature	medium
train speed	<=39
number of tracks	1
track inspection intervals	4 weeks
track type	switch and crossing
lineside object density	low
lineside object type	anchored
location of track	In tunnel
rolling stock inspection interval	1 week
driver experience	high
competence of rolling stock maintainer	high
competence of infrastructure maintainer	high
track fault type	gauge spreading
track fault severity	high
S&C fault severity	high
type of obstruction	large animals
rolling stock fault type	brake failure
rolling stock fault severity	medium

Table C-4: Conditions relating to a typical location on the GB rail network, for use in the validation of the output of the fault tree section of the BN

The fault tree base event probabilities calculated by the BN when entering the evidence in Table C-4 were:

Event 1: 0

Event 2: 0.000225

Event 3: 0.43003

Event 4: 5.0 e^{-05}

Event 5: 0.9998

Event 6: 0

Event 7: 0.000499

Event 8: 0.000349

Event 9: 0

Event 10: 0.0014

Event 11: 1

Event 12: 5.0 e^{-07}

Event 13: 0.00062

Event 14: 0.074

Event 15: 0.9999

Event 16: 5.0 e^{-07}

Event 17: 0.07179

Event 18: 0.000507

Event 19: 0.9999

Event 20: 0

Event 21: 0.25

Event 22: 0.1739

Event 23: 0.002

Event 24: 0.025

Event 25: 0.0147

Both the BN (bn fault tree validation 3.hkb) and the fault tree (bn fault tree validation 3.psa) calculated a top event probability, for gate 1, of 1.404e-07.

C.9.4 Comparison of model output with output of SRM version 4

The SRM model includes occurrence rates for precursors – causes of accidents. Precursor probabilities are not representative of their probability of occurrence in any particular identifiable location – they are network average occurrence rates per track mile. Therefore, it is not possible to structure the BN model, or add evidence into it, so that the assumptions that underpin it are consistent with those that underpin the precursor rates. However, in order to gauge whether the output of the BN model is plausible its output, given certain assumptions, can be compared against the network average figure. To allow such a comparison to be made, we need to map the precursors to events in the BN model.

The table below shows which combinations of hazardous events could be considered to relate to event/gate occurrence rates in the BN.

BN gate	Equivalent hazardous events (taken from SRM version 4.0)
Gate 2 – over speed derailment occurs	Running into large animals leading to train derailment, Overspeeding leading to PT derailment, Severe braking/snatch leading to PT derailment, **Total rate of occurrence = 8.11E-10 per track mile per year**
Gate 3 – track fault derailment occurs	Buckled rail leading to PT derailment, Broken rail leading to PT derailment, Broken fishplate leading to PT derailment, Broken rail in tunnel leading to PT derailment, Track twist leading to PT derailment, Track maintenance staff errors leading to PT derailment, Incorrect scotch and clip of points leading to PT derailment. **Total rate of occurrence = 1.41E-08 per track mile per year**
Gate 13 – S&C (Switch and Crossing) derailment occurs	Other driver/train crew error at S&C leading to PT derailment, Shunter errors leading to PT derailment, SPAD at S&C leading to PT derailment, Wrongside signal failure at S&C leading to PT derailment, Defective S&C leading to PT derailment, Points in the wrong position and not detected leading to PT derailment, Movement of points under train (equipment faults) leading to PT derailment. **Total rate of occurrence = 9.69E-09 per track mile per year**
Gate 17 – rolling stock fault derailment	Seized axle box bearing leading to PT derailment, axle failure leading to PT derailment, Suspension system/bogie failures leading to PT derailment, Wheel flats or wheel/tyre wear beyond limits leading to PT derailment, Wheel failure leading to PT derailment. **Total rate of occurrence = 1.47E-09 per track mile per year**
Gate 21 – obstruction derailment	Running into items that have fallen onto the line leading to train derailment, Running into trees leading to train derailment, Running into items placed on the track by vandals leading to train derailment, Cat D SPAD or runaway leading to PT derailment, Running into Engineers materials left foul leading to train derailment, Running into to debris from overbridges leading to train derailment, Running into debris from lineside structures/buildings leading to train derailment, Running into landslip leading to train derailment, Subsidence/ landslip under track leading to PT derailment, Running into debris in the tunnel leading to train derailment, Running into objects fallen from trains leading to PT derailment, Running into vehicles fallen from overbridge leading to train derailment, Running into vehicles through boundary fence leading to train derailment, Running into snow/ice leading to train derailment. **Total rate of occurrence = 3.17E-08 per track mile per year**

Table C-5: Mapping of precursor occurrence rates to BN gate occurrence probabilities

The condition states shown in Table C-1 were entered into the BN, and the evidence propagated through the net. The probabilities calculated for the five gates inputting to the top event, derailment occurs, were compared with their equivalents from the SRM. The two sets of probabilities are shown in Table C-6.

BN gates	Probability per track mile per year, calculated using BN model with the condition states shown in Table C-1 set.	Probability per track mile per year, calculated by aggregating relevant precursor rates (see Table C-5).
Gate 2 – over speed derailment occurs	4.50e-10	8.11E-10
Gate 3 – track fault derailment occurs	1.16e-08	1.41E-08
Gate 13 – S&C (Switch and Crossing) derailment occurs	4.60e-09	9.69E-09
Gate 17 – rolling stock fault derailment	1.12e-9	1.47E-09
Gate 21 – obstruction derailment	9.19e-08	3.17E-08

Table C-6: Comparison of derailment probabilities calculated by the BN, with equivalent probabilities calculated with the SRM

We can see that the probabilities of occurrence for gates 2, 3, 17 and 21 are all lower than their SRM equivalents. This is a sensible finding, as the SRM figure does not represent the likelihood of a derailment at an average location, it represents the average likelihood of a derailment.

(This thesis argues that there are 'hotspots' on the network. These 'hotspots' would be expected to inflate the network average. We would therefore expect that the likelihood of a derailment at an average location would in fact be lower than the network average)

The probability of a derailment due to a switch and crossing fault is higher than the network average figure. This too is understandable. The SRM figure is an average per track mile. If we take into account the fact that there might only be S&C in place, on average for 1 track mile in every 40 miles of track then the estimate calculated by the BN would need to be divided by 40 in order to make a more meaningful comparison. This would give a figure of 1.19e-09, again a figure below the network average.

It should be remembered that, in the absence of a full set of data the BN model has been developed with a limited data set, supported by judgement – essentially guesswork. Therefore, the model cannot be considered to be a fully validated risk model suitable for use in real risk management problems. Nevertheless these

validation exercises show that the logic captured in the fault and event tree models has been effectively implemented in the BN, and that the output from the model is plausible.

Appendix D Industry feedback on use of the approach

A copy of the letter received from:

Stuart Parsons, CMIOSH, MIIRSM, Programme Manager – Safety Management Systems, Rail Safety & Standards Board;

providing his feedback on the thesis and the new risk modelling approach it proposes is available from the author on request.